МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

(Минобрнауки РД)

П Р И К А З

«01» февраля 2024 г. № 08-02-1-64/24

Махачкала

О проведении Республиканского информационного часа в образовательных организациях

С целью формирования у обучающихся образовательных организаций Республики Дагестан критической оценки к информации, распространяемой в информационно-телекоммуникационной сети «Интернет»,

ПРИКАЗЫВАЮ:

1. Организовать и провести с 5 по 16 февраля 2024 г., далее – постоянно, в образовательных организациях Республики Дагестан Республиканский информационный час.

2. Руководителям общеобразовательных организаций, подведомственных Министерству образования и науки Республики Дагестан:

2.1. Организовать с участием представителей правоохранительных органов проведение классных информационных часов для обучающихся (далее – классные часы) с применением информационно-наглядных материалов (приложение № 1).

2.2. Провести родительские собрания «Родители и дети – вместе в сети «Интернет» (далее – родительские собрания) с обсуждением информационно-наглядных материалов (приложение № 3).

2.3. Информацию о проведенных классных часах и родительских собраниях размещать на официальных страницах образовательных организаций Республики Дагестан в информационно-телекоммуникационной сети «Интернет».

2.4. Разместить на информационных стендах образовательных организаций информационно-наглядные материалы (приложения № 1 и № 3).

3. Руководителям образовательных организаций среднего профессионального образования, подведомственных Министерству образования и науки Республики Дагестан, организовать для обучающихся информационный кураторский час с применением методических рекомендаций для педагогов и родителей (законных представителей) обучающихся по развитию навыков критического мышления обучающихся, позволяющих противостоять манипулятивным воздействиям средств массовой информации и сети «Интернет», вовлекающим подростков в протестную деятельность (далее – кураторский час) (приложение № 2).

4. Руководителям общеобразовательных организаций и образовательных организаций среднего профессионального образования, подведомственных Министерству образования и науки Республики Дагестан, в срок до 27 февраля 2024 г. представить на адрес электронной почты: zarina.d@dagminobr.ru информацию о проведенных классных часах, кураторских часах и родительских собраниях по форме согласно приложению № 4 к настоящему приказу.

5. Государственному бюджетному учреждению дополнительного профессионального образования Республики Дагестан «Дагестанский институт развития образования» (Ахмедова Г.А.):

5.1. В период с 1 марта 2024 г. по 30 марта 2024 г. организовать и провести для педагогов образовательных организаций курсы повышения квалификации на тему «Формирование кибербезопасного поведения обучающихся в социальных сетях» (далее – курсы).

5.2. В срок до 5 апреля 2024 г. на адрес электронной почты: zarina.d@dagminobr.ru представить информацию о проведенных курсах с указанием сведений о педагогах, принявших участие в курсах, в разрезе муниципальных образований Республики Дагестан.

6. Руководителям муниципальных органов управления образованием, образовательных организаций среднего профессионального образования Республики Дагестан рекомендовать реализацию мероприятий, указанных в пунктах 2-4 настоящего приказа.

7. ГКУ РД «Информационно-аналитический центр» (Ибрагимов А.Х.) разместить настоящий приказ на официальном сайте Министерства образования и науки Республики Дагестан в информационно-телекоммуникационной сети «Интернет».

8. Контроль за исполнением настоящего приказа возложить на заместителя министра Магомедова Г.М.

Министр **Я. Бучаев**

Приложение № 4
к приказу Минобрнауки РД

«01» февраля 2024 г. № 08-02-1-64/24

Информация
о проведенных классных часах, кураторских часах и родительских собраниях в образовательных организациях

аименование ГО/СПО/ ОО, едомственной инобрнауки РД	Количество проведенных, информационных классных часов (кураторских часов) в МУО/СПО/ ОО, подведомственной Минобрнауки РД	Количество приглашенных специалистов с указанием сферы деятельности	Общий охват обучающихся, принявших участие в информационных классных часах (кураторских часах)	Количество родительских собраний, проведенных в МУО/СПО/ ОО, подведомственной Минобрнауки РД	Количество родителей, принявших участие в родительских собраниях	Ссылки в сети «Интернет» на проведенные мероприятия

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНСТИТУТ РАЗВИТИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПЕДАГОГОВ И РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) ОБУЧАЮЩИХСЯ ПО РАЗВИТИЮ НАВЫКОВ КРИТИЧЕСКОГО МЫШЛЕНИЯ ОБУЧАЮЩИХСЯ, ПОЗВОЛЯЮЩЕГО ПРОТИВОСТОЯТЬ МАНИПУЛЯТИВНЫМ ВОЗДЕЙСТВИЯМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ И СЕТИ ИНТЕРНЕТ, ВОВЛЕКАЮЩИХ ПОДРОСТКОВ В ПРОТЕСТНУЮ ДЕЯТЕЛЬНОСТЬ

Протестная деятельность

ПРОТЕСТ- субъективное переживание личностью угрозы потери благ, свободы, достоинства и ценностей и проявляется в виде устойчивых личностных особенностей или ситуативных реакций, направленных на устранение этой угрозы

Конвенциональные форма протеста

легальные и регулируемые законом

Неконвенциональная форма протеста

создание экстремистского контента в «социальных сетях»;
участие в неразрешенных демонстрациях и митингах;
участие в акциях гражданского неповиновения;
участие в захватах зданий, предприятий; блокирование дорожного движения;
участие в насильственных и террористических акциях и др.

Протест как деструктивный показатель внутриличностного и межличностного конфликтов, выражения своих интересов и потребностей

Высокая протестная активность у подростков

СКЛОННЫ К

проявлению физической, косвенной, вербальной агрессии, идеализации и индивидуализму

СТРЕМЯЩИЕСЯ К

критичности и самокритичности при отсутствии знаний и умений применять их на практике; новыми идеями и иногда зависимы от авторитетов

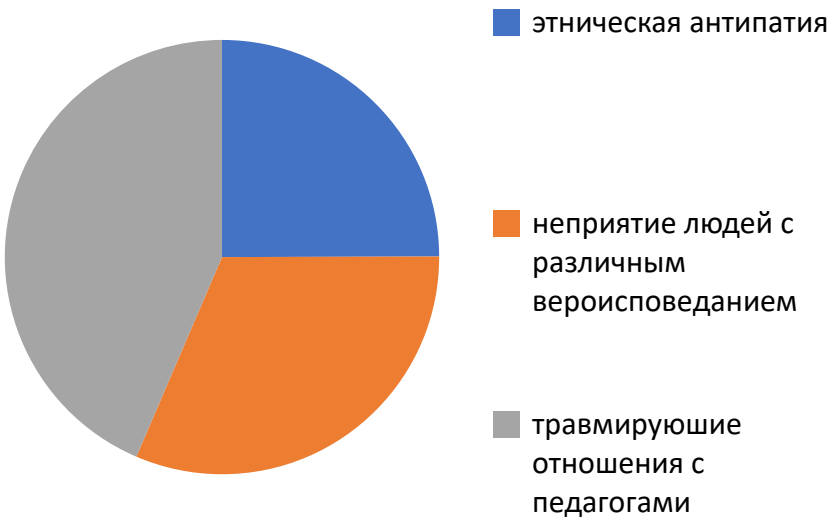
ИМ ПРИСУЩИ

раздражительность, обида, чувство вины, подозрительность, эмоциональная незрелость

ПРОЯВЛЯЮТ

ответственность, чувство долга и достоинства, независимость, активность в отстаивании своих позиций и идей; склонность к соперничеству и доминированию.

Подростки, входящие в группу риска
(М.А. Одинцова и М.В. Тищенко)



СМИ и сеть Интернет как средства манипуляции подростками

Средства массовой информации (СМИ) и сеть Интернет)

Пресса (газеты, журналы), книжные издательства, телевидение, радиовещание, кино-видео-звукозапись

Интернет, социальные сети - ВКонтакте, Facebook, Одноклассники, Twitter, Instagram,

МАНИПУЛЯЦИЯ - это психологическое и информационное воздействие на отдельного человека или группу (объект управления) для изменения мышления и поведения вопреки интересам и желаниям.

Роли манипуляторов в Интернете

– «френды» – втираются в доверии, вводят в заблуждение, обманывают;
– «тролли» (тролли-профессионалы) – намеренно разжигают в дискуссии отрицательные эмоции;
– «диктаторы» – повелевают, заставляют;
– «судьи» (наставники) – дают советы, наставляют, обличают;
– «жертвы» («прилипалы») – просят о помощи, жалуются, втираются в доверие;
– «защитники» – демонстрируют свою поддержку и помощь в решении проблем.

Манипуляторов в Интернете определяем по их действиям

ОНИ

– требуют внимания к себе, играя роль жертвы, человека с проблемами и пр.;
– угрожают и обвиняют, создают дискомфорт, вызывают чувство страха;
– иронизируют, используя слабые места пользователя,
– обвиняют, тем самым развивают чувство вины;
– лицемерят, ведя интриги;
– заставляют сомневаться в собственной адекватности, подменяя смыслы.

Психологические механизмы манипуляции, используемые в Интернете (Д.Г. Трунов)

1 ВОЗДЕЙСТВИЕ НА ЭМОЦИОНАЛЬНОЕ СОСТОЯНИЕ ПАРТНЕРА

Так, например, освещение информации в негативном ракурсе будет способствовать проявлению запредельных эмоциональных реакций агрессии у адресной аудитории

2 МАНИПУЛИРОВАНИЕ РЕСУРСАМИ

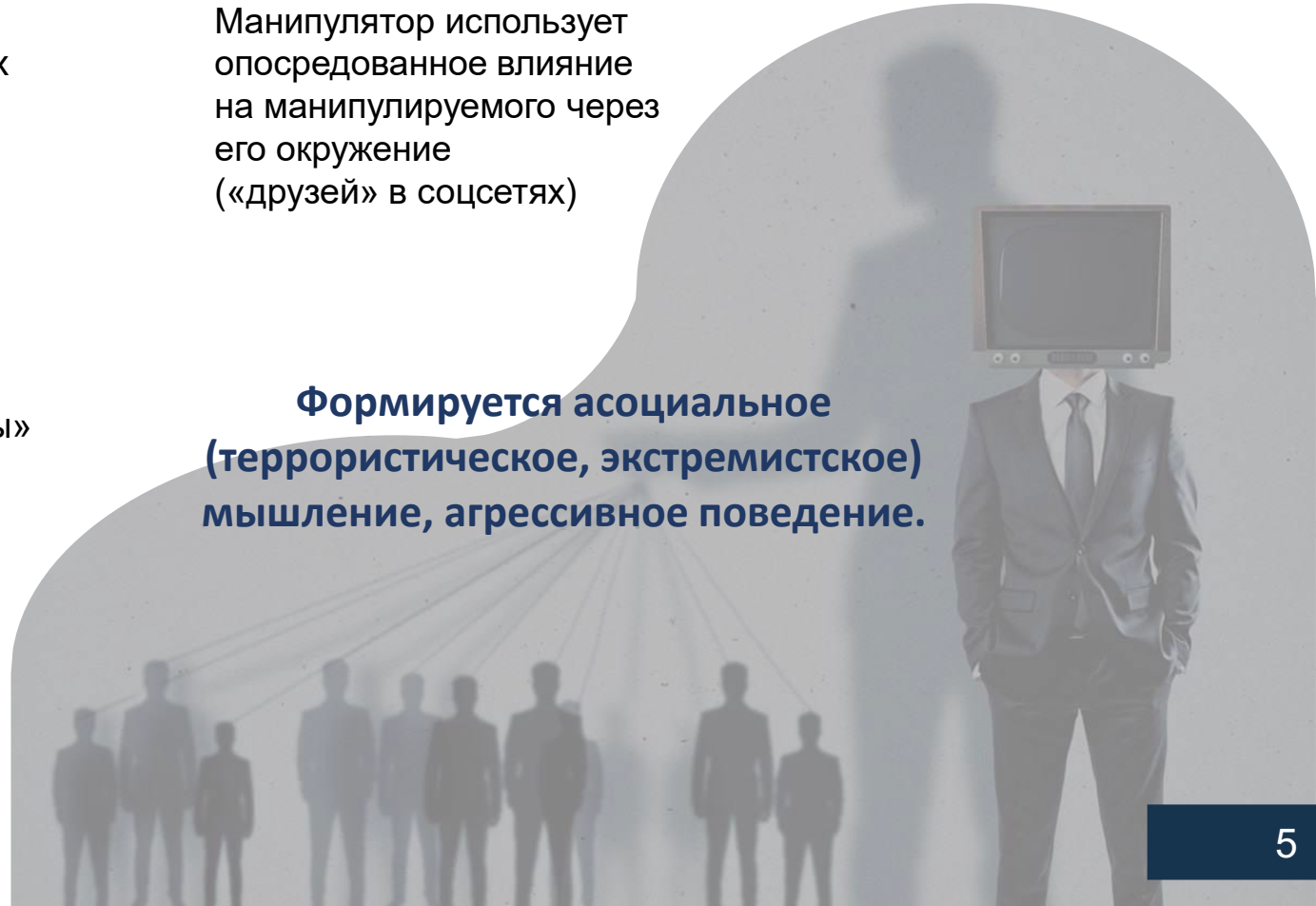
В среде интернет-коммуникаций особенную роль имеет статус: количество подписчиков, рейтинг, оценки и др. В таком случае манипулятор может использовать «ресурсы» своего аккаунта для получения необходимого результата

3 ЭКСПЛУАТАЦИЯ ЛИЧНОСТНЫХ ОСОБЕННОСТЕЙ ОБЪЕКТА МАНИПУЛЯЦИИ

Манипулятор использует в первую очередь в своих целях личностные особенности пользователей, их потребности, интересы, ценности, привычки, чувства

4 ИСПОЛЬЗОВАНИЕ ВЗАИМООТНОШЕНИЙ

Манипулятор использует опосредованное влияние на манипулируемого через его окружение («друзей» в соцсетях)



Формируется асоциальное (террористическое, экстремистское) мышление, агрессивное поведение.

Понятие и особенности критического мышления

Критическое мышление

Тип мышления для решения нетривиальных практических проблем, оно направлено на понимание и осмысление полученной информации. Оценочное и рефлексивное мышление.

Способность человека сомневаться во входящей информации и своих убеждениях, мыслить ясно и рационально, искать логическую связь между фактами и формулировать сильные аргументы

наблюдение, анализ, вывод (интерпретация), связь, решение проблем, саморегуляция (оценка и рассуждение)

НАВЫКИ

мыслить самостоятельно; работать с информацией как основой для анализа и сравнения; мыслить проблемно и аргументированно, используя обоснованные доводы, утверждения и доказательства; применять критическое мышление в социальном аспекте

УМЕНИЯ

критика и самокритика

Основные понятия

Составляющие критического мышления

Основные характеристики критического мышления (Д. Клустер)

- Критическое мышление является самостоятельным мышлением. Оно носит индивидуальный характер, так как каждый человек формулирует свои идеи, оценки и убеждения независимо от остальных. Критическое мышление не обязано быть совершенно оригинальным. Человек вправе принять идею или убеждение другого человека как свои собственные, что подтверждает его правоту;
- информация является отправным, а не конечным пунктом критического мышления. Знание создает мотивировку, без которой человек не может мыслить критически;
- критическое мышление начинается с постановки вопросов и уяснения проблем, которые нужно решить, оно следует за проблемным мышлением и переплетается с ним;

- Критическое мышление является аргументированным. Аргументация состоит из трех основных элементов: утверждение (тезис, основная идея, положение), довод и доказательство. Наличие иных точек зрения (контраргументов) усиливает аргументацию. Критически мыслящий человек, вооруженный сильными аргументами, способен противостоять авторитетам;
- Критическое мышление является социальным мышлением. Любая мысль проверяется и оттачивается, когда ею делятся с другими.

Развитие навыков критического мышления обучающихся на учебных занятиях

Развитие критического мышления обучающихся зависит от их

- способности уверенно ориентироваться в излагаемом материале, не принимать безоговорочно на веру предлагаемую информацию, умении оценить степень ее истинности и соотнести с тем, что известно, осмыслено и принято;
- открытости по отношению к новой информации, нестандартным способам решения как известных, так и новых задач, стремлении к познанию нового и неизвестного;
- готовности и умения вести конструктивный диалог с преподавателями, родителями и друзьями;
- способности провести многомерный анализ и осмысление внешней информации;
- готовности к самодиагностике в отношении сформированности различных умений и качеств на основе сравнения собственных результатов с заданным эталоном и т. д.

Этапы учебного занятия по развитию критического мышления

1. Вызов
2. Осмысление и формулировка проблемы
3. Размышление и рефлексия
4. Самоанализ, самокоррекция
5. Обобщение и оценка, самооценка.

Методы и методики развития критического мышления

МЕТОДЫ

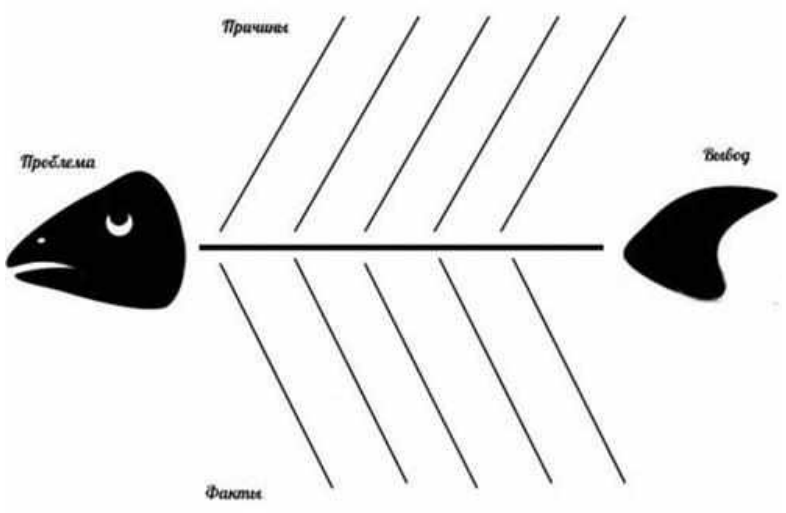
Проблемная дискуссия
Перекрёстная дискуссия
Интернет-дискуссия
Дискуссия по «технике аквариума
Межгрупповой диалог
Дебаты

МЕТОДИКИ

«5W+H» - система вопросов, с помощью которых следует проверять всю входящую информацию
IMVAIN - метод проверки источников
«Мозговой штурм» - создания какой-либо идеи, проекта, обсуждения темы

Фишбоун – методический прием развития навыков критического мышления (Д. М. Шакирова)

Развивает умения обучающихся анализировать и классифицировать информацию из текста, выделять основные события и искать их причины, обобщать и делать выводы, участвовать в дискуссии, критически оценивать себя и аргументы других, приводить логические доказательства, находить несоответствия.



- Голова – проблема, вопрос или тема, которые подлежат анализу.
- Косточки, расположенные сверху, – на них фиксируются основные понятия темы, причины, которые привели к проблеме.
- Косточки, расположенные снизу, – факты, подтверждающие наличие сформулированных причин или суть понятий, указанных на схеме.
- Хвост – ответ на поставленный вопрос, выводы, обобщения.

ФГБОУ ДПО ИРПО разработаны методические рекомендации по организации работы по профилактике участия несовершеннолетних в массовых протестных акциях (митингах)

https://firpo.ru/

1. Методические рекомендации для педагогов и родителей (законных представителей) обучающихся по профилактике социальных рисков, связанных с манипулятивным воздействием средств массовой информации и сети интернет
2. Методические рекомендации для родителей (законных представителей) по профилактике противоправного поведения несовершеннолетних и их участия в протестном движении
3. Методические рекомендации для педагогов по организации профилактической работы, направленной на недопущение участия несовершеннолетних в несанкционированных акциях и митингах
4. Методические рекомендации для педагогов и родителей (законных представителей) обучающихся по развитию навыков критического мышления обучающихся, позволяющего противостоять манипулятивным воздействиям средств массовой информации и сети интернет, вовлекающих подростков в протестную деятельность
5. Методические рекомендации для педагогов по развитию навыков участия в конструктивных дискуссиях, направленных на противостояние манипулятивным воздействиям средств массовой информации и сети интернет, вовлекающих подростков в протестную деятельность

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНСТИТУТ РАЗВИТИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»

ЦЕНТР СОДЕРЖАНИЯ И ОЦЕНКИ КАЧЕСТВА СПО

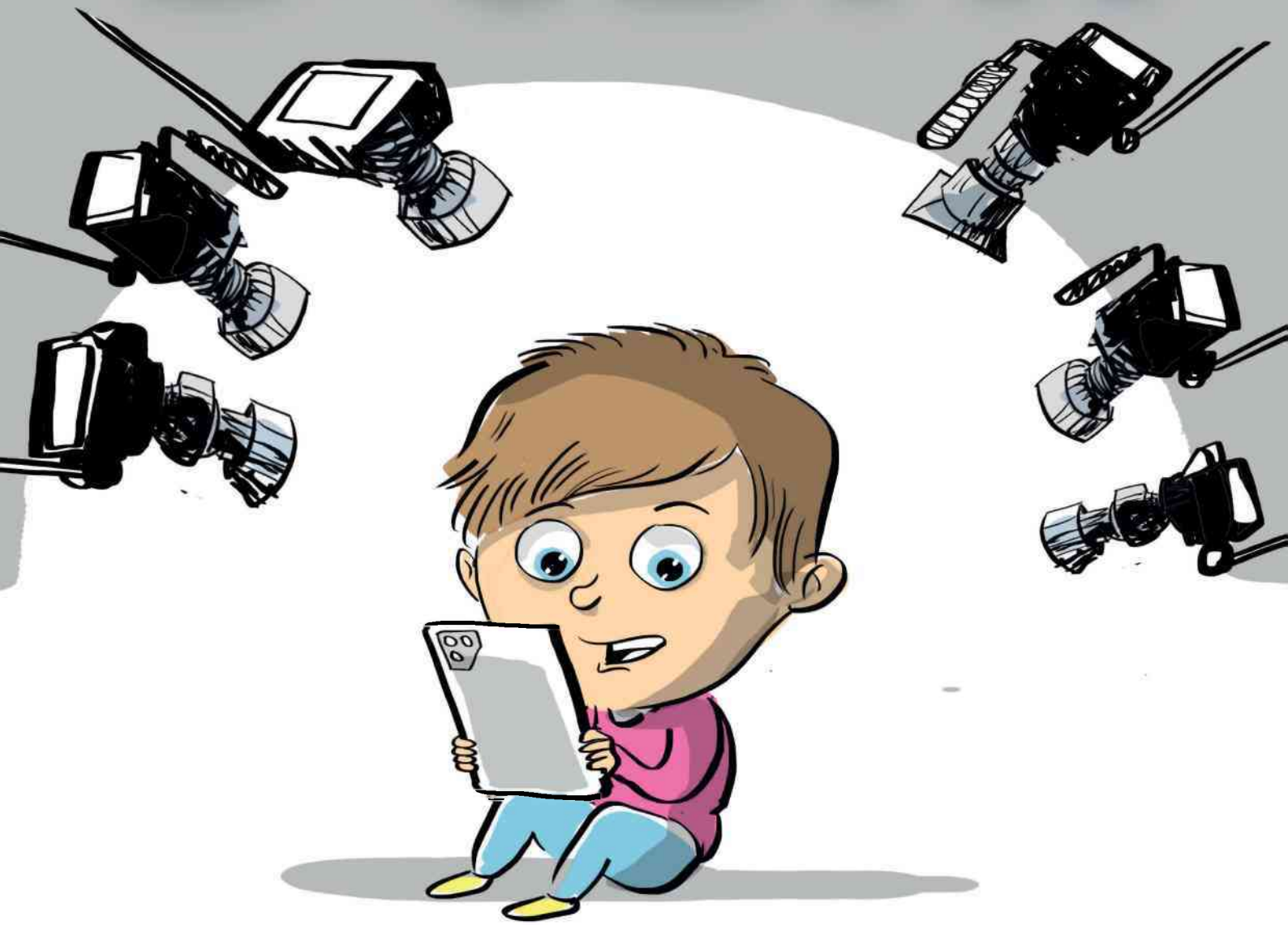
НАУЧНО-МЕТОДИЧЕСКИЙ ОТДЕЛ

Составитель: Шашенкова Елена Анатольевна, к.п.н., доцент, начальник НМО

cams@firpo.ru

Научно-методический отдел
тел. раб.: +7 (915) 499-64-48

АНОНИМНОСТЬ В СЕТИ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

Возможна ли анонимность в сети? Многим до сих пор не дает покоя этот вопрос, но на него есть однозначный ответ.

АНОНИМНОСТЬ В СЕТИ – МИФ!

Многим людям до сих пор кажется, что Интернет – безопасное и абсолютно анонимное место, где каждый может писать и делать все, что ему вздумается. Но это не так. Поэтому тебе следует помнить две важных истины:

1. **Всё, что однажды попало в Интернет, остаётся там навсегда.**
2. **В Интернете можно найти кого-угодно, даже если пользователь попытался скрыть о себе всю информацию.**

Многие пытаются скрыть свою личность в Интернете. Например, простые пользователи делают это, чтобы друзья или близкие не узнали о каких-то их увлечениях. Но гораздо чаще это делают хулиганы или преступники, которым важно, чтобы их действия остались в тайне. Они боятся проблем с законом и пользуются различными способами: создают фейковые профили в соцсетях, используют специальные программы-анонимайзеры.

Однако следует помнить, что каждое твое действие в Интернете содержит информацию о том устройстве, с которого ты это делал – например о телефоне или компьютере. А твой Интернет-провайдер видит все, что ты делаешь в Интернете несмотря на любую программу. Следовательно, эта информация может быть доступна кому угодно: от сотрудника полиции до преступника.

> **Важно помнить, что Интернет – это такое же публичное пространство, как улица, парк или школа. Там действуют те же правила – общайся прилично, соблюдай правила вежливого поведения и относись к другим людям так же, как хочешь, чтобы относились к тебе.**

Ведь каждое действие или грубость в Интернете может иметь последствия. **Клевета и оскорбление являются противоправными деяниями, за совершение которых предусмотрена ответственность.** Уважай других людей, относись с пониманием и состраданием к чужой беде. Научись ставить себя на место другого человека. А также больше времени проводи в реальном мире, общаясь с друзьями по-настоящему, а не в сети.

АНОНИМНОСТЬ В СЕТИ – МИФ!

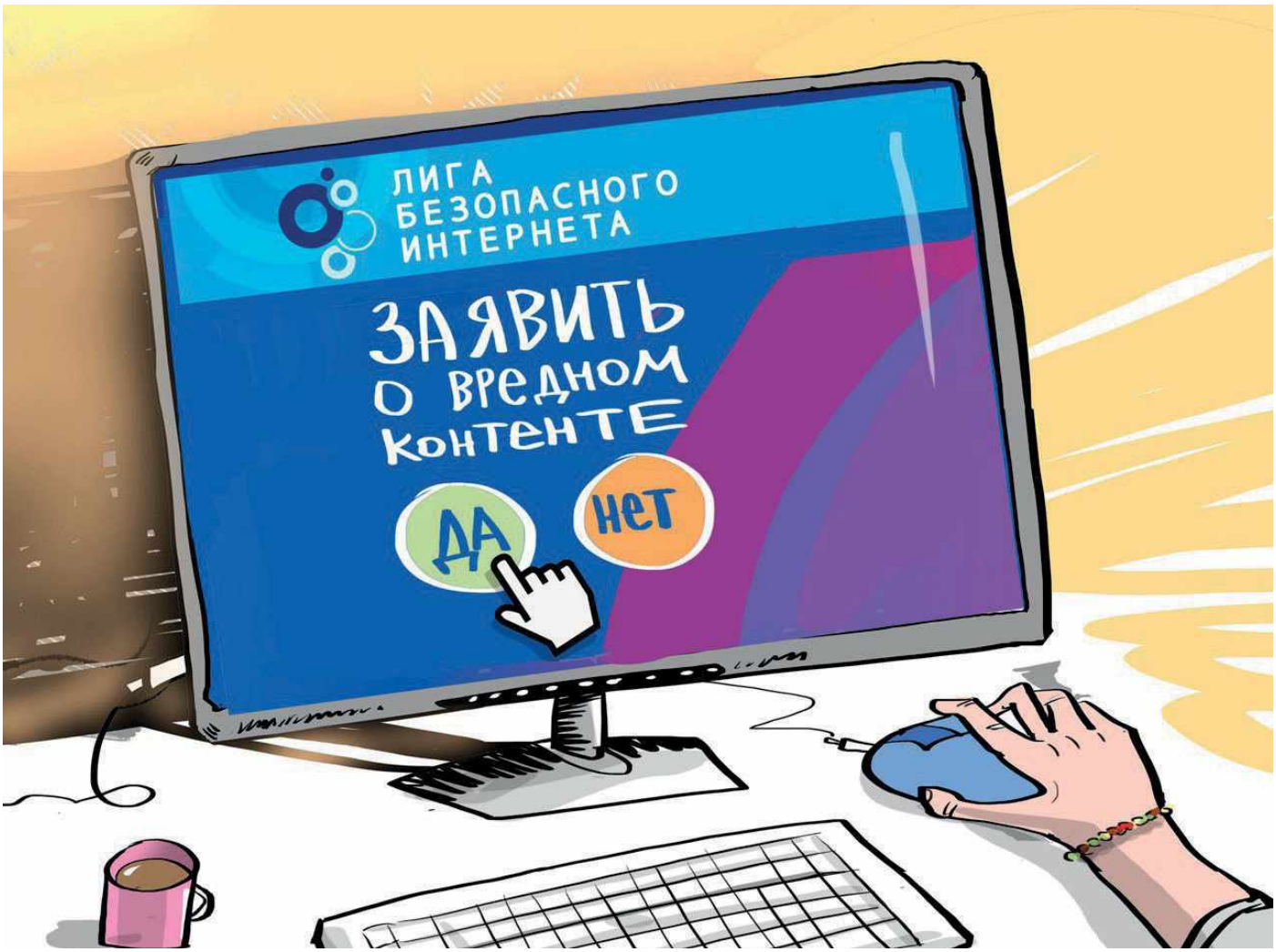
ОПАСНЫЕ ПУБЛИКАЦИИ В СОЦИАЛЬНОЙ СЕТИ: ПОЧЕМУ НЕЛЬЗЯ ПРОМОЛЧАТЬ!

Ваше право повлиять на Интернет

Многие из вас сталкиваются с опасным контентом в соцсетях. Такой контент может принимать самые разные формы. В опросе, проведенном ВЦИОМ, 32% опрошенных заявили о вреде, который Интернет приносит обществу, 35% согласились, что контент в Интернете может нести угрозу семейным ценностям, а 46% отметили, что Интернет значительно увеличивает число самоубийств.

> Здесь дана подробная инструкция по обращению в органы власти в связи с распространением деструктивного контента. Инструкция универсальна и применима ко всем социальным сетям. Направление обращений в органы власти — это ваше право по закону. **Никто не может вас в этом ограничить.**

В обращении указывается конкретная ссылка на аккаунт, группу, сообщество, чат или список таких ссылок. Желательно также прикладывать скриншоты самих публикаций, так как часто они бывают удалены/заблокированы/скрыты к моменту рассмотрения письма.



Ключевой вопрос:

Куда и к кому обращаться по поводу опасной информации в сети?

Внимание!

Вы установили факты распространения детской порнографии, призывов к суициду, рекламы азартных игр (онлайн-казино), склонения несовершеннолетних к противоправным действиям. По всем этим темам нужно обращаться в Роскомнадзор.

Сделать это можно двумя способами:

- **Первый:** если у вас есть аккаунт на госуслугах, то проще направить через приложение Роскомнадзора. Вы можете скачать его в магазине приложений как для Android, так и для Apple:

https://play.google.com/store/apps/details?id=org.rkn.ermp
https://apps.apple.com/us/app/ркн/id1511970611

В приложении необходимо приложить ссылку и скриншот опасной публикации. Здесь очень быстро можно отследить результат обращения, проверить был ли заблокирован тот или иной ресурс.

- **Второй:** если нет учетной записи на госуслугах, то можно направить через форму на официальном сайте Единого реестра запрещённых сайтов:

https://eais.rkn.gov.ru/feedback/

Здесь необходимо выбрать тему обращения, прикрепить ссылку и скриншот опасной публикации.

Надо знать!

Наркотики, экстремизм:

Если кто-то в видео или публикации пропагандирует наркотики, говорит об эффектах от их употребления или демонстрирует употребление, то нужно обращаться в Министерство внутренних дел Российской Федерации. Для этого на сайте МВД России необходимо выбрать Главное управление по контролю за оборотом наркотиков.

Также в МВД России необходимо обращаться, если вы столкнулись с информацией экстремистского характера, в том числе с контентом, посвященным скулшутингу (массовые расстрелы в школах). Для этого на сайте МВД России необходимо выбрать Главное управление по противодействию экстремизму.

Чаще всего это довольно агрессивные публикации с использованием нецензурной брани, где содержатся призывы убивать, громить, крушить, истреблять, использовать оружие, физическую силу, выходить на улицы для применения насилия, нападать на группы людей или социальные учреждения.

Форму для подачи заявления вы можете найти на официальном сайте МВД России:

https://мвд.рф/request_main

На сайте необходимо заполнить данные и вставить текст письма. В тексте необходимо добавить ссылку на публикацию и указать название соцсети и прикрепить скриншот.

ЛГБТ-пропаганда, видеоролики с насилием, жестокостью, истязанием людей или животных, пропаганда проституции и аморального образа жизни, информация, вызывающая у детей страх, ужас или панику, видео ненасильственных смертей и катастроф:

Подача заявления по такому контенту осуществляется на официальном сайте Генеральной Прокуратуры Российской Федерации:

https://epp.genproc.gov.ru/web/gprf/internet-reception

Введите текст обращения и прикрепите скриншот опасной публикации. Необходимо также добавить ссылку на публикацию и указать название социальной сети.

Также, обращения о фактах нарушения Российского законодательства в Интернете можно присылать Лиги безопасного Интернета: info@ligainternet.ru или передавать по горячей линии: 8 (800) 700-56-76. Лига безопасного Интернета перенаправляет все входящие обращения в соответствующее ведомство.

Не опускайте руки!

ВОПРОС: «Я направил/а обращение и получил/а ответ, в котором содержится отказ в рассмотрении или опасная информация не была обнаружена».

ОТВЕТ: Любой ответ, содержащий отказ в рассмотрении обращения, либо отказ в удалении противоправной информации, вы можете обжаловать в прокуратуре. Инструкция по обращению в прокуратуру дана выше. К письму необходимо приложить сканы/копии ответов с отказом.

Также вы можете такие ответы присылать нам, в Лигу безопасного интернета. В дальнейшем мы перенаправим их в Роскомнадзор, МВД или Генеральную прокуратуру и будем добиваться удаления информации.

Ответы вы можете присылать на почту info@ligainternet.ru с пометкой «Отказ». Если вы хотите публиковать ответы в комментариях, то не забывайте закрывать на скриншотах ваши персональные (личные) данные!

Личный пример

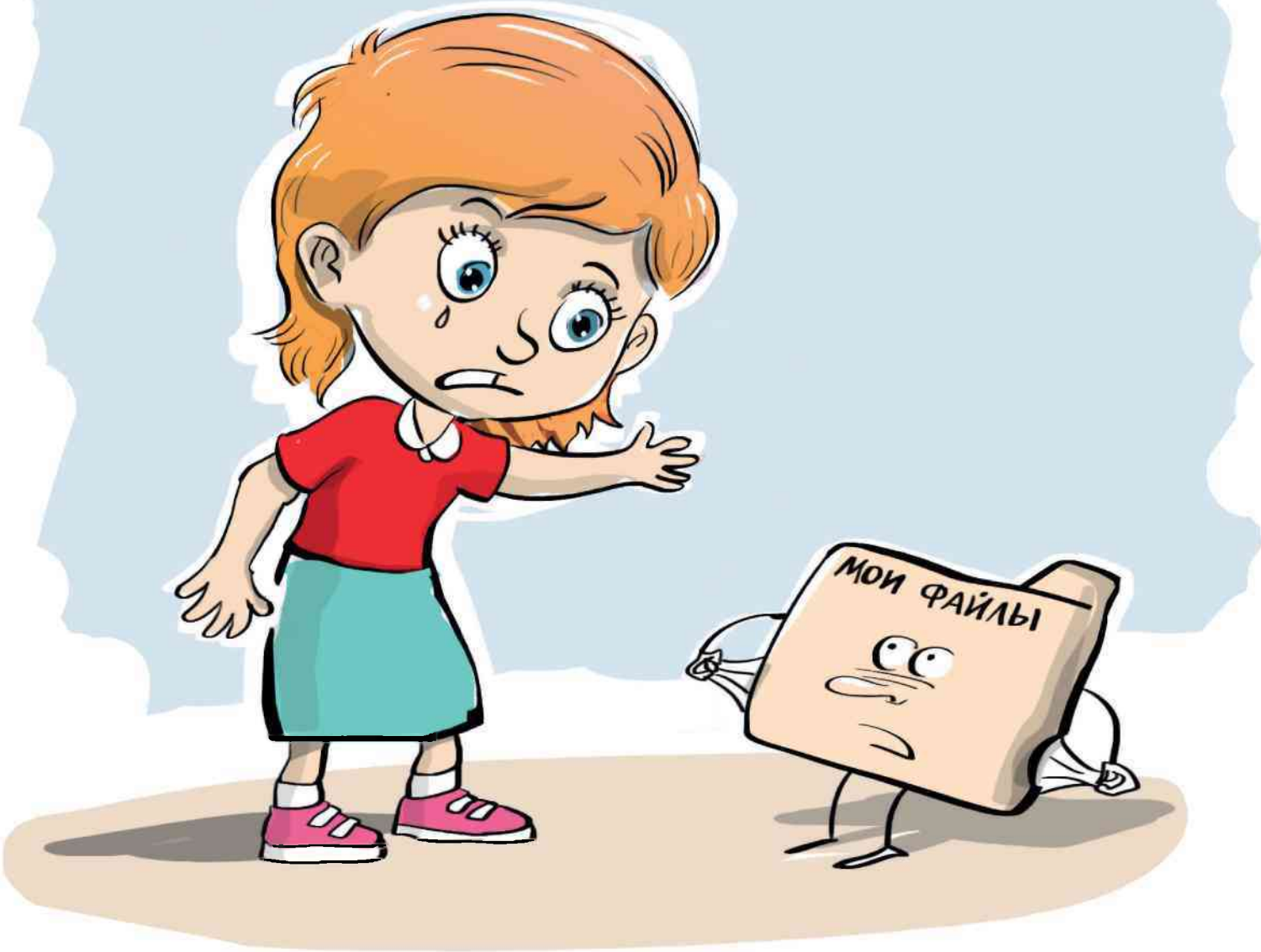
Чем больше обращений будет подано, тем быстрее социальные сети будут очищены от противоправного контента.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

Персональные данные – это все ключевые и важные сведения о человеке. Их следует тщательно беречь и не раскрывать в Интернете без необходимости. Раскрытие персональных данных в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже аккаунтов, мошенническим действиям, вымогательству денег у тебя или твоих близких, угрозах совершения компрометирующих тебя действий, краже денег и документов. В некоторых случаях это даже может привести преступника на порог твоего дома.

Что относится к персональным данным?

1. **Фамилия, имя, отчество;**
2. **Все твои документы** (паспорт, свидетельство о рождении, аттестат и др.);
3. **Банковские данные** (номер счета, карты, пин-код, CVV-код);
4. **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
5. **Фотографии и видеозаписи с твоим изображением;**
6. **Данные о твоих родственниках;**
7. **Твои логины и пароли.**

Чаще всего пользователи сети сами выкладывают информацию о себе в Интернет. Мошенники охотятся за этими данными. Большинство информации о жертвах преступники находят в открытом доступе в соцсетях и в Интернете.

Как защитить свои персональные данные?

1. **Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов.** Пароль восстановить проще, чем вернуть украденные деньги.
2. **Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**
3. **Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.
4. **Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.
5. **Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.
6. **Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.

МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!

КАК ГАРАНТИРОВАТЬ СВОЮ БЕЗОПАСНОСТЬ В СЕТИ

Сложное слово, простые правила

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Ваш цифровой след хорошо виден! О каждом пользователе Интернета ежедневно собирается и хранится огромное количество информации. В основном ее собирают социальные сети и мессенджеры. Делается это для того, чтобы как можно точнее идентифицировать каждого пользователя и показывать ему наиболее актуальную рекламу. Чем точнее реклама попадает в интересы и увлечения пользователя, тем больше шансов, что он поддастся на нее, купит товар или приобретет услугу. Однако вся эта информация может попасть в руки к мошенникам. По данным ВЦИОМ, 57% получают звонки от телефонных мошенников, 19% получают от них сообщения, а 9% россиян потеряли деньги в результате действий мошенников.

Ключевой вопрос: Как обеспечить кибербезопасность?

Внимание!

Мошенники могут испо льзовать ваши данные самыми разными способами:

- Продать их другим мошенникам;
- Втереться в доверие и использовать для вымогательства денег;
- Использовать для шантажа;
- Использовать для травли.

Полезные советы

1. **Следите за галочками** (разрешениями), которые ставите (даёте сайтам и приложениям). Иногда кнопка «Ок», появившаяся на экране, означает полный доступ к вашему микрофону, камере или телефонной книге. Таким же образом, вы можете неосторожно оформить подписку на ненужную вам услугу или установить ненужные, а иногда и опасные программы на компьютер. Будьте бдительны!
2. **Старайтесь не пользоваться бесплатными сервисами.** Большинство бесплатных сервисов и приложений, включая мессенджеры и VPN-плагины, могут предоставлять свои услуги на бесплатной основе. Если программа доступна бесплатно, следует задуматься, чем же зарабатывают ее разработчики. Как правило – это персональные данные пользователей программы, которые она ежедневно записывает и передает разработчикам. Те же, в свою очередь, продают их сторонним организациям.
3. **Помните,** что все ваши публикации в Интернете не только публичны, но и хранятся вечно. Помните! Любая приватность может быть нарушена, публикации могут стать доступны в случае утечки.
4. **Не публикуйте и не отправляйте материалы интимного характера.** Любая информация, которую вы выкладываете в Интернет, может стать поводом для шантажа, провокации, а в будущем может даже принести проблемы в карьере. Материалы интимного характера, даже в переписках, не удаляются из Интернета и могут быть использованы преступниками для изготовления порнографических материалов с целью последующей продажи или фальсификации компромата. Никогда не отправляйте фото и видео интимного характера даже самым близким людям, поскольку всегда существует вероятность утечки информации из-за неосторожности, взлома почты или аккаунта.
5. **На незнакомые сайты лучше даже не заходить.** Некоторые сайты способны самостоятельно устанавливать вредоносные программы и вирусы. Для этого даже не нужно ничего скачивать, достаточно просто зайти на сайт. То же относится к письмам и сообщениям, которые приходят из незнакомых источников.
6. **Ненадежные и сомнительные письма лучше не открывать** и уж тем более нельзя скачивать файлы, пришедшие от неизвестного отправителя в письмах или мессенджерах. Это относится даже к текстовым файлам. Например, файлы формата .pdf, в котором распространяется большинство документов, вполне способны распространять вирусы среди скачавших пользователей.

Личный пример

Не публикуйте в соцсетях лишнюю информацию о себе. Абсолютно вся информация, включая ваши фото, адреса, увлечения, имена домашних животных и многое другое, могут быть использованы мошенниками для установления личности, создания подробной картины о вас, как о пользователе, и подбора персональных мошеннических схем.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

КИБЕРУГРОЗЫ: ЗНАНИЕ О ФАКТОРАХ ОПАСНОСТИ – ВАША БЕЗОПАСНОСТЬ!

Ключ в виртуальный мир

Современный смартфон – полноценный персональный компьютер. Он обладает всеми теми же функциями, что и домашний компьютер или ноутбук, а в чем-то даже их превосходит. В отличие от домашнего компьютера смартфон имеет постоянный доступ в Интернет, он работает 24 часа в сутки, имеет продвинутую камеру и микрофон, а также датчики движений, что позволяет ему круглосуточно записывать всю информацию о своем пользователе. Так, смартфон является нашим ключом в виртуальную реальность.

Ключевой вопрос

Как сделать свой смартфон безопасным?

Источники проблемы

- **Огромное количество навязчивой рекламы** – сайты, приложения, соцсети и игры – все это содержит огромное количество рекламы, на которой зарабатывают их разработчики. По данным Всероссийского центра изучения общественного мнения 29% россиян получают спам ежедневно.
- **Информационный шум** – в цифровом мире множество неконтролируемых уведомлений, которые приходят на телефон практически ежеминутно. Большинство пользователей не хотят тратить время на их отключение и удаление. А они содержат часто совсем ненужные рекламные предложения, приманки и являются способом вымогательства денег пользователя.
- **Установка нежелательного и вредоносного программного обеспечения** – при переходе по новой ссылке, скачивании файлов, установке приложений (даже из проверенных источников!) существует вероятность установки вирусов, шпионских или рекламных программ. Опасность могут представлять даже приложения, скачанные из официальных магазинов смартфонов. По данным ВЦИОМ, лишь 16% родителей устанавливают на устройство их ребенка антивирус.
- **Утечка персональных данных владельца** – все, что содержится в смартфоне, начиная от логинов и паролей, заканчивая фотографиями, банковскими реквизитами и даже перепиской, может не только попасть в руки к мошенникам, но и стать достоянием общественности.

Внимание!

Чем активнее используется устройство, тем больше данных о своем владельце оно накапливает. К таким данным относятся не только ваши фото, видео, переписки, но и такие данные, как:

- история установки и использования приложений;
- история энергопотребления, то есть циклов и времени зарядки, интенсивности работы;
- история уведомлений и действий;
- история магазина приложений;
- история браузера;
- история перемещений по городу и многое другое.

Надо знать!

Вредоносные приложения на смартфонах пытаются заработать на пользователе – вытянуть деньги, внимание пользователя, показывая ему рекламу или перенаправляя на сайты, украсть персональные данные или профиль пользователя, передать мошенникам доступ к самому устройству.

Вредоносные приложения бывают разными:

- **Фальшивые приложения** – копия настоящих приложений, как правило, банковских или приложений мобильных операторов. Их задача – полностью замаскировавшись под настоящее приложение, украсть у пользователя данные от личного кабинета и получить доступ к мобильному или банковскому счету.
- **Приложения-вымогатели** – блокируют устройство и требуют перечисление денег за разблокировку.
- **Денежные «пиявки»** – программы со скрытой подпиской. Однажды купив подобную программу или совершив покупку с её помощью, можно обнаружить, что она оформила «полноценную» подписку и деньги теперь списываются регулярно. Как правило, всегда можно отказаться от «денежной пиявки» и отменить такую подписку. Следите за своими расходами в сети.

Информация к размышлению

Вредоносные программы можно разделить на две большие категории:

- **Вирусы** – вредоносные программы, которые напрямую вредят устройству, установленным программам. Распространяются по Интернету и заражают устройства.
- **Трояны** – маскируются под настоящие программы, а иногда даже могут выполнять некоторые полезные функции. Похищают данные пользователя, рассылают спам, создают трафик на сайты.

Как вирусы попадают на устройство?

- **Из зараженного электронного письма** или файла, приложенного к письму – нельзя открывать письма, пришедшие из неизвестных источников, а особенно скачивать и запускать файлы, прикрепленные к этим письмам. Вирусы могут распространяться даже через текстовые файлы, например в формате .pdf.
- **Через зараженный сайт** – многие сайты способны самостоятельно устанавливать на компьютеры вирусы. Для этого бывает достаточно просто открыть страницу. Это особенно актуально для нелегальных сайтов, например, с пиратским контентом.
- **Через установку неизвестных приложений** с неизвестного сайта – если вы скачиваете что-либо из Интернета, убедитесь, что источник надежен. Программы лучше скачивать с официальных сайтов разработчиков этих программ.

Как защитить себя от киберугроз:

- **Не открывайте письма и сообщения от незнакомых отправителей;**
- **Не скачивайте пиратский контент;**
- **Внимательно проверяйте адреса веб-сайтов**, которые вы посещаете;
- **Не устанавливайте на телефон или компьютер, приложение из непроверенного источника;**
- **Не давайте приложениям разрешения, которые не нужны им для работы** – приложению «калькулятор» не нужен доступ к микрофону смартфона;
- **Следите за своими расходами в сети** и за тем, какие подписки оформляют приложения;
- **В настройках телефона отключите уведомления** от приложений, которые вы не хотите получать;
- **Установите на компьютер и телефон антивирус;**
- **Храните на телефоне как можно меньше информации о себе.** Так вы защититесь от утечки данных;
- **Подключите на телефоне функцию защиты от спама**. На некоторых устройствах она доступна в настройках или ее можно подключить у мобильного оператора.

Личный пример

Не открывайте MMS и сообщения, присланные с незнакомых номеров!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru

ОБЩЕНИЕ С НЕЗНАКОМЦАМИ ОНЛАЙН: ПОЧЕМУ ЭТО ОПАСНО

Агрессоры в цифровом мире

Одна из самых больших опасностей в сети – люди, которые по разным причинам могут представлять угрозу для здоровья или психики ребенка. Такие люди зачастую угрожают не только детям, но и взрослым.

Кто представляет в Интернете наибольшую угрозу

- **Тролли и агрессоры.** Интернет-травля иногда носит организованный характер, когда группа обидчиков координирует свои действия и может даже иметь единый «центр управления».
- **Шантажисты.** Если информация или материалы личного характера попадают в руки к злоумышленникам, они могут использовать их для шантажа своей жертвы.
- **Вербовщики.** Эти люди ищут среди пользователей сети тех, кого смогут приобщить к каким-то определенным идеям, группам или движениям, зачастую носящим криминальный или экстремистский характер.
- **Манипуляторы.** Воздействуют на эмоции и психику широкой группы пользователей с целью вызвать у них агрессивное поведение или спровоцировать на какие-то действия.
- **Мошенники.** Стремятся похитить у пользователя его персональные данные или финансовые средства. С этой целью используют методы социальной инженерии, манипулируют эмоциями жертвы, а также прибегают к техническим средствам, подделывая сайты, профили и даже номера телефонов.
- **Педофилы.** Входят в доверие к ребенку, иногда маскируясь в Интернете под другого ребенка. Обманом навязывают ему встречу или заставляют его присылать материалы интимного характера.

Ключевой вопрос

Что такое «Нежелательный контакт»?

Внимание!

Нежелательным контактом называется любое общение в Интернете, беспокоящее вашего ребенка, создающее конфликтную ситуацию или обстоятельства, при которых ему может быть причинен вред. Также в сети ребенок может столкнуться с опасными или неуместными материалами, способными расстроить, напугать или обидеть его. 82% детей получают запросы на дружбу в социальных сетях от незнакомых людей, а 29% - от незнакомых взрослых (по данным Лаборатории Касперского)

Ребенку следует остерегаться незнакомцев в Интернете, которые:

- Задают много вопросов о его личной жизни.
- Просят об одолжениях в обмен на что-либо.
- Просят никому о них не рассказывать.
- Пытаются контактировать с ребенком множеством различных способов – смс, соцсети, онлайн-чаты и т.п.
- Задают ребенку вопросы о том, кто еще имеет доступ к его телефону, компьютеру или аккаунту.
- Лестно отзываются о внешнем виде ребенка.
- Задают вопросы или делают комментарии личного или интимного характера. 10% детей отмечали, что им приходили странные сообщения от взрослых пользователей.
- Настаивают на личной встрече. 37% детей встречаются с теми, с кем познакомились онлайн.
- Заставляют ребенка чувствовать себя виноватым или угрожают ему.

Полезные советы

- Расскажите детям, что делать, если им пишет кто-то, с кем они не хотят общаться.
- Уберите учетные записи детей из публичного доступа.
- Настоятельно посоветуйте ребенку удалить контакты людей, с которыми он не знаком лично.
- Договоритесь с детьми, какие данные они могут публиковать в Интернете, а какие нет. Например, фотографии, место жительства, учебы и т.д.
- Ребенку постарше предложите сделать страницы в соцсетях закрытыми для посторонних и подробно изучить настройки конфиденциальности, чтобы он мог контролировать, кто именно будет видеть его фотографии и записи.
- Лучший способ избежать опасного общения в сети – заблокировать человека, который пытается контактировать с ребенком и пожаловаться на его аккаунт администрации соцсети.
- Если вы поймете, что преследование ребенка со стороны незнакомых лиц, его травля или вовлечение в депрессивно-суицидальный контент не прекращаются, а все возможные меры помощи исчерпаны, следует сменить аккаунт ребенка, мобильное устройство и номер его телефона. Желательно на какое-то время полностью исключить ребенка из Интернета, например, пойти в поход с ребенком на несколько дней куда-нибудь, где не будет зоны покрытия сети.

Это надо знать!

Очень важно объяснить ребенку, что «виртуальные друзья» должны оставаться виртуальными, но если ребенок хочет встретиться с кем-либо из них, то вы хотели бы, чтобы он делал это с вашего разрешения. Безопаснее всего встречаться днем, в общественном месте и в сопровождении родителей или кого-либо из взрослых, кому ребенок доверяет.

Объясните ребенку, что он должен как минимум ставить кого-нибудь из родителей в известность о том, куда он направляется и с кем собирается встретиться.

Что делать, если ребенок попал в опасную ситуацию?

- Сохраняйте спокойствие и заверьте ребенка, что его никто не собирается ругать.
- Объясните ему, что даже взрослых иногда обманом заставляют делать то, о чем они потом жалеют.
- Дайте ребенку понять, что он всегда сможет обсудить с вами любой вопрос, не боясь наказания или критики.
- Не лишайте ребенка доступа в Интернет. Это может быть воспринято как наказание, и в дальнейшем ребенок не захочет рассказывать вам о своих проблемах.
- **Если вы считаете, что жизни или здоровью ребенка угрожают, сообщите об этом в полицию по номеру 102.**
- Прежде чем блокировать кого-либо или удалять записи, обязательно заснимите и сохраните доказательства – фото или скриншоты переписок, даты и время записей, ссылки на публикации или аккаунты.
- **Если эти материалы включают в себя интимные изображения детей младше 18 лет, имейте в виду, что хранение и распространение таких изображений является преступлением. Обязательно обратитесь в полицию.**

Личный пример

Обсудите с детьми, как они могут реагировать на различные раздражающие ситуации. Они должны понять, что в любой момент могут поговорить с вами, довериться, получить помощь!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

10 СОВЕТОВ ДЛЯ ДЕТЕЙ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

1. **Для развлечения и общения с настоящими друзьями Интернет не нужен, нужна реальная жизнь**. Сокращай время пользования Интернетом! Отводи для общения в виртуальном мире не более 1 часа в день. Не позволяй социальным сетям отбирать у тебя здоровье и перспективы!

2. **Анонимность в сети - миф. Всё, что мы выкладываем в Интернете, остаётся там навсегда.**

3. **Проводи больше времени в реальной жизни:** общайся с друзьями, родителями, найди себе действительно интересное увлечение, читай, занимайся спортом, придумывай и реализуй полезные социальные проекты, помогай людям, включайся в общественную деятельность, смелее используй свои таланты.

4. **Будь бдителен! В Интернете много мошенников, которые охотятся за твоими деньгами и данными.** Есть и такие преступники, целью которых является испортить как можно больше детей или загубить их жизнь. Некоторые делают это за большие деньги, продавая снимаемые детьми видео и фотографии, а некоторые потому, что психически больны. Однако понять это, общаясь в Интернете, невозможно. Просто не подпускай к себе незнакомых людей и не позволяй им сделать из тебя свою жертву.

5. **Не выкладывай свои персональные данные в Интернет!** Помни, что отправлять их не стоит даже друзьям.

6. **Закрой свои страницы в соцсетях от посторонних!** Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и не продолжай общение.

7. **Не бойся рассказать родителям о своих проблемах!** Если кто-то решит тебя обижать, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.

8. **Помни, что из Интернета ничего не удаляется!** Если ты не хочешь, чтобы какие-то твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.

9. **Не верь всему, что написано в Интернете!** В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.

10. **Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни.** Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

НЕ СЛЕДУЙ МОДЕ!

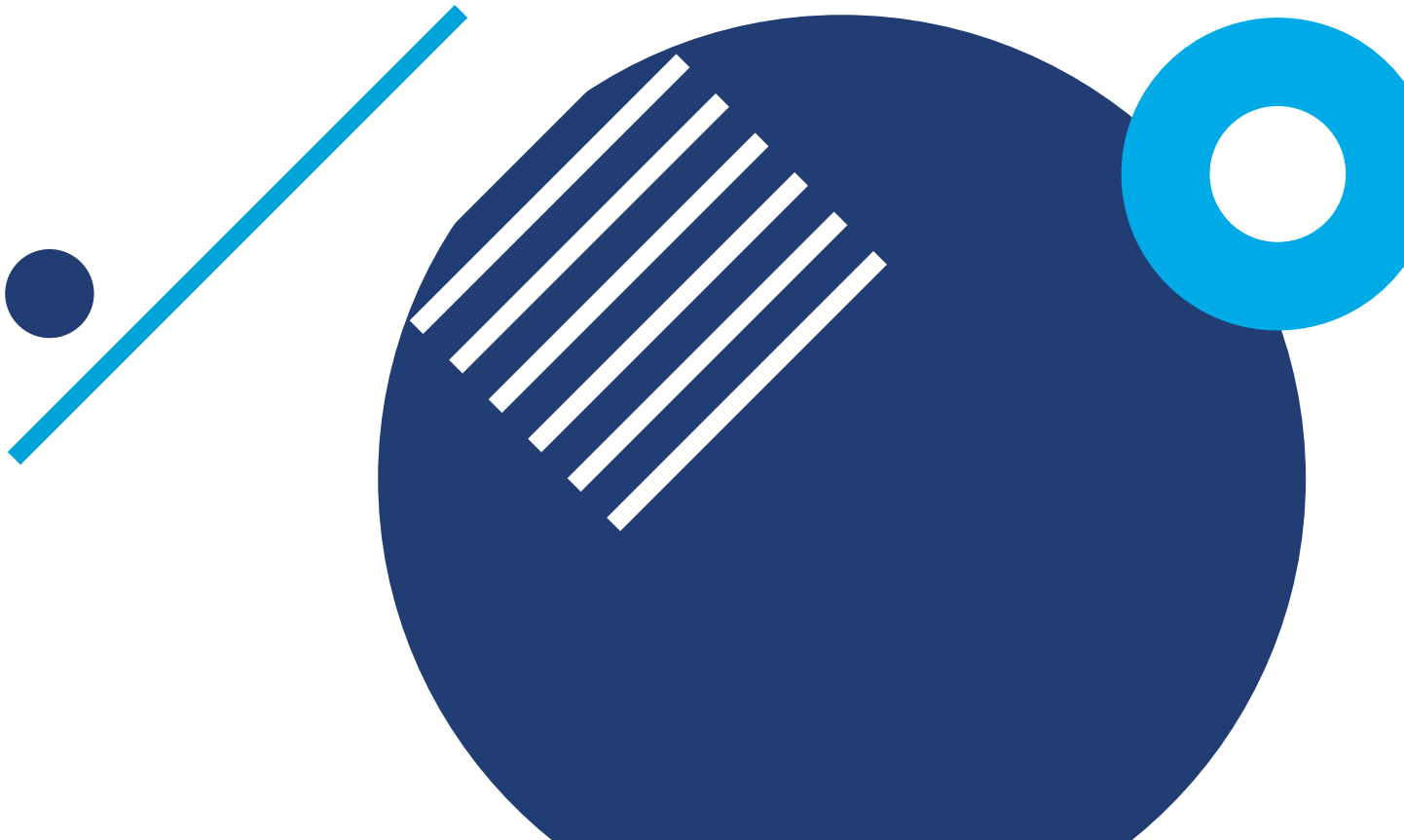
Социальные сети – самый верный способ «убить время». Сетевые развлечения поглощают его без остатка. Но с головой погружаясь в виртуальный мир, мы забываем про друзей, близких, учебу, работу, активный отдых и развитие.

Тебе может показаться, что не иметь профиля в социальной сети – это странно, но на самом деле все вовсе не так. Если у тебя нет профиля в соцсети – поздравляем! Ты уже победил! Ведь теперь у тебя будет гораздо больше времени на полезные вещи: учебу, спорт, настоящую, не сетевую дружбу!

Все больше россиян признаются, что соцсети приносят им больше негативных эмоций: печаль, обиду, зависть. Отказ от соцсетей поможет стать по-настоящему счастливым.

Современные соцсети созданы не для общения. Они созданы для рекламы, для продажи товаров и услуг, навязывания чужого мнения. А если у тебя нет соцсетей – ты мыслишь и думаешь самостоятельно!

НЕ ПОГРУЖАЙСЯ В ИНТЕРНЕТ С ГОЛОВОЙ! ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!



ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЦЕНИМ И УМЕЕМ СОХРАНЯТЬ!

Что надо знать о персональных данных

Персональные данные – все данные о человеке, своего рода «паспорт его личности». Их следует тщательно беречь и не раскрывать в Интернете без необходимости. В противном случае это может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям. Безопасность – это наша непререкаемая ценность для детей и взрослых!

Что относится к персональным данным?

1. Фамилия, имя, отчество;
2. Номера и реквизиты всех документов (паспорт, СНИЛС, ИНН, свидетельство о рождении, аттестат об образовании, медицинский полис и т.п.);
3. Банковские данные (номер счета, карты, пин-код, CVV-код и т.п.);
4. Ваша контактная информация (номера телефонов, адреса электронной почты, адреса жительства, работы или учебы);
5. Фотографии и видеозаписи с вашим изображением;
6. Данные о ваших родственниках;
7. Ваши логины и пароли.

Ключевой вопрос:

Насколько реально и как сохранить персональные данные вашей семьи?

Внимание!

Более трети россиян (37%) не знают, для чего и как могут быть использованы персональные данные (по данным ВЦИОМ)!

Соцсети, мессенджеры и видеохостинги ежедневно собирают о нас огромное количество данных. Делается это, в первую очередь, для заработка денег. Большинство крупных платформ – бесплатны, ведь их владельцы зарабатывают на своих пользователях. Точнее – на их персональных данных, при перепродаже или использовании в рекламе. Соцсети и мессенджеры берут эти данные не только из профиля пользователя, но и из его переписки. Обратите внимание: вся переписка постоянно хранится на серверах социальной сети или мессенджера, поэтому в результате утечки, кражи или хакерской атаки ваша частная жизнь может стать достоянием общественности.

Источники беды

Не стоит надеяться на «приватные» публикации, просматривать которые может только ограниченный круг лиц, которых настраивает сам пользователь. Ведь утечка может произойти через любого из этих людей. Иногда происходят крупные утечки, в результате чего данные тысяч пользователей попадают в открытый доступ. Но чаще всего пользователи сами выкладывают информацию о себе в Интернет. Защитите себя и свою семью! 80% информации о жертвах преступники находят в социальных сетях (по данным Роскомнадзора).

Кроме персональных данных о каждом человеке собираются также его фото- и видеоизображения. Современного человека ежедневно снимают сотни видеокамер, расположенных в публичных местах. Эта информация собирается, в первую очередь, государственными органами с целью обеспечения безопасности, раскрытия преступлений и т.п. Однако следует помнить, что такие видеозаписи могут попасть и в руки к шантажистам или иным злоумышленникам. Будьте осторожны! Не помогайте мошенникам, добровольно передавая им персональные данные.

В текущей ситуации большинство порталов органов власти и коммерческих компаний становятся объектами хакерских атак в ежедневном режиме.

Так, за последнее время в публичный доступ утекли базы данных пользователей компании «Яндекс.Еда» и клиентов медицинской лаборатории «Гемотест». Все это происходит из-за того, что в России до сих пор нет существенной административной и уголовной ответственности для операторов подобных баз. Так, «Яндекс.Еда» «отделалась» штрафом всего лишь в 60 тысяч рублей.

Важно помнить, что из-за халатности или экономии компании на хранении данных, которые мы оставляем, оформляя карточку в магазине, на заправке или любом другом месте могут стать достоянием общественности.

Надо помнить!

Активный пользователь Интернета оставляет цифровой след – иногда свой полный портрет: состояние здоровья, внешность и физические данные, привычки, места пребывания, уровень дохода, данные о личной и интимной жизни и многое другое. Приложения на телефоне могут получить доступ микрофону, камере, акселерометру (используется для измерения движений устройства) и следить за своим пользователем круглосуточно. Всё это может представлять интерес для преступников! Мошенничество, шантаж, травля – вот неполный список того, для чего злоумышленники могут использовать информацию о пользователях. Следите за культурой поведения в сети, сохраняйте свою частную жизнь и конфиденциальность!

В соответствии с действующим законодательством любой гражданин вправе отказаться от предоставления своих персональных данных. Согласие на обработку персональных данных может быть отозвано гражданином у организации в любой момент.

Если вас принуждают к подписанию согласия на обработку персональных данных и отказывают в предоставлении услуги, смело обращайтесь в прокуратуру.

Полезные советы

1. Посоветуйте своему ребенку при регистрации в социальных сетях использовать только имя или псевдоним (никнейм).
2. Следите за тем, чтобы ребенок не размещал в интернете лишнюю информацию: где он живет, где учится, какой дорогой ходит на уроки и т.п.
3. В настройках камеры на телефоне следует отключить геотеги (геолокацию, место съемки). Эта функция показывает, где именно делалась фотография. В таком случае любой желающий по фото может отследить пользователя.
4. Полезно будет настроить приватность в аккаунте своего ребенка. Таким образом его профиль смогут смотреть только его друзья.
5. Объясните ребенку, что нельзя выкладывать в Интернет фото или скан-копии его документов или банковских карт.
6. Расскажите ребёнку, что персональными данными стоит делиться только с ограниченным кругом лиц – самыми близкими. Не стоит передавать такие данные друзьям, а особенно незнакомым людям из соцсетей.
7. Ребёнку надо знать, что злоумышленники могут пытаться выведать информацию и персональные данные через личные сообщения в социальных сетях. Особенно внимательно стоит реагировать на ссылки, которые незнакомцы присылают ребёнку в личных сообщениях. Лучше по ним не переходить, а неизвестные файлы – не открывать.
8. Расскажите ребенку, что нельзя подключаться к первому попавшемуся бесплатному Wi-Fi в публичном месте. Через такую бесплатную сеть злоумышленники могут получать доступ к персональным данным пользователей.

Личный пример

Тщательно отбирайте фото и видео, которые вы сами выкладываете в Интернет!

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: необходимые средства защиты

Процветающий бизнес на каждом из нас

Современные технические средства очень сильно изменили виды мошенничества, которые используются злоумышленниками. Они могут, например, подделывать сайты, создать страницу абсолютно идентичную странице Интернет-магазина с нужным вам товаром, но при оплате деньги отправятся напрямую к мошенникам.

Самым распространенным способом мошенничества в Интернете является «фишинг». С его помощью мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу, например, известной соцсети. При попытке войти в свой профиль на таком сайте мошенники получат полный доступ к вашему аккаунту.

Они с лёгкостью подделывают любой номер телефона и не только его цифры, но даже могут сделать так, что при звонке ребёнок увидит надпись, например, «полиция», «мама», «брат» и т.п. Более половины россиян регулярно получают звонки от мошенников (по данным ВЦИОМ). Страшно? Есть способы остановить злоумышленников!

Ключевой вопрос

Как противостоять преступным действиям мошенников?

Внимание!

Современные мошенники активно используют социальную инженерию – психологические приемы, вынуждающие жертву сделать именно то, что нужно мошеннику, например перейти по ссылке, скачать вредоносный файл или сообщить код из СМС. По данным ВЦИОМ, 9% россиян теряли деньги в результате действий Интернет-мошенников, а 6% заявляли о краже крупных сумм.

За чем же охотятся цифровые мошенники?

- **Деньги;**
- **Персональные данные;**
- **Логины и пароли.**

Надо запомнить!

1. Для современных мошенников персональные данные являются не менее ценными, чем денежные средства, а иногда они даже полезнее. Именно с помощью персональных данных преступники отнимают у жертвы денежные средства, входя к ней в доверие. Кроме того, персональные данные сами по себе имеют ценность, ведь мошенники могут продавать их другим преступникам.
2. Кроме онлайн-мошенников существует другая, не менее опасная группа – телефонные мошенники. Они могут представиться кем угодно: сотрудником банка, полиции, прислать СМС от имени родственника. Они также используют социальную инженерию, пытаясь украсть данные. Иногда мошенники специально охотятся за голосом человека, например, задавая навязчивые вопросы. Их интересует то, как абонент назовет свои ФИО, а также скажет: «Да». В дальнейшем мошенники могут использовать записи голоса для входа в банковский аккаунт жертвы, голосом подтверждая банковские операции.
3. Еще одна опасность в Интернете – скрытые платные подписки. Многие мошенники или недобросовестные организации провоцируют пользователей на оформление подписок таким образом, что пользователь узнает об этом только тогда, когда обнаружит регулярное списание денег со своего счета. Такую скрытую подписку можно случайно оформить при переходе на сайт с пиратским контентом, при скачивании файла или приложения или при оплате какой-либо услуги в Интернете. Так, например, однократно купив что-либо или пожертвовав деньги, можно не заметить галочку, которая подтверждает ваше согласие на подписку. Иногда создатели сайта специально делают эту галочку едва различимой или даже вовсе скрытой с экрана. Будьте бдительны!

Полезные советы

Как защитить ребенка от мошенничества в Интернете?

1. В первую очередь следует научить ребенка перепроверять информацию. В случае с сайтами следует обращать внимание на адресную строку – нет ли в адресе сайта каких-либо изменений или неточностей. Если адрес отличается от настоящего даже на один символ – это явный признак подделки. Если входящий звонок поступает от представителя банка или другой структуры, следует самостоятельно перезвонить в эту организацию и задать им вопрос, есть ли у них такой сотрудник и мог ли он вам сейчас звонить. Чаще всего банки не осуществляют операции по звонкам. Однако следует учитывать, что мошенники могут целиком скопировать даже настоящий номер и представиться настоящим именем сотрудника.
2. Объясните ребенку, что не следует принимать поспешных решений. Мошенники могут требовать от жертвы принять решение в текущий момент. Они рассчитывают на то, что в спешке, панике или страхе человек утратит бдительность и охотнее согласится на перевод денег. В таком случае можно ответить: «Сейчас я все проверю и перезвоню вам», или «перезвоните мне через 5-10 минут, мне нужно время, чтобы подумать». Обычно этого времени хватает человеку, чтобы распознать мошенников, проверить информацию и не допустить ошибки.

3. Ребенка следует приучить беречь свои персональные данные с раннего возраста. Ребенок должен знать, что именно относится к персональным данным и что их нельзя размещать в Интернете без необходимости. Опасность представляют как сами данные, так и фотографии документов. Даже простое размещение номера телефона в социальной сети может привести к нежелательным звонкам, спаму, угрозам или шантажу.
4. Если у ребенка уже есть банковская карта, не следует хранить на ней много денег. Лучше всего класть деньги на карту тогда, когда он собирается что-то потратить или хранить на ней небольшое количество денег, которое не страшно будет потерять.
5. Не привязывайте телефон ребенка к банковским картам, счетам, платежным системам. Все платежи за ребенка лучше проводить самостоятельно.
6. Ограничивайте установку приложений на телефон ребенка. Наличие на телефоне антивируса и родительского контроля позволит защитить телефон от спама и вредоносных программ.
7. Установите ограничения и контроль на мобильном счете ребенка. Лимит расходов, можно установить в личном кабинете мобильного оператора. Там же можно отключить возможность оформления платных подписок и изменения тарифа.
8. Научите ребенка опасаться звонков с незнакомых номеров и не перезванивать на них. К любому звонку с неизвестного номера следует относиться с осторожностью. Если перезвонить на такой номер, вас могут перевести на линию, где за каждую минуту разговора с вашего счета будут списываться огромные деньги.
9. Объясните ребенку, что нельзя переходить по ссылкам из СМС и загружать файлы, которые пришли с неизвестного номера. Такой файл или ссылка могут установить на устройство вирус или отправить все данные владельца телефона прямо в руки к мошенникам.
10. Подключите ребенку защиту от нежелательных звонков. Такая функция есть у смартфонов на системах Android и iOS. Она позволит отфильтровать спам, звонки с опасных и нежелательных номеров.
11. Если ребенок уже стал жертвой мошенников, следует немедленно обратиться в полицию. Не забудьте сохранить все доказательства мошеннической деятельности – скриншоты сайтов, переписок, квитанции онлайн-платежей.

Личный пример

Установите на смартфоне ребенка надежный пароль, который он должен знать наизусть и ни с кем не делиться. Это обезопасит устройство при попадании в руки чужих людей, в том числе других детей.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

КЛИПОВОЕ МЫШЛЕНИЕ: ЦЕНА ДЛЯ ЛИЧНОСТИ

Небезопасные клипы

Клиповое мышление – тип мышления, заключающийся во фрагментарном восприятии информации. Люди с преобладающим клиповым мышлением склонны к восприятию информации отрывочно и порционно, небольшими кусками, при этом значительно страдает глубина понимания материала, а также критический подход к информации.

У современных подростков такой тип мышления преобладает. Его формированию активно способствует формат подачи информации в соцсетях, особенно короткие видео (в TikTok, YouTube).

Особенности клипового мышления:

- Фрагментарность;
- Яркость;
- Кратковременность;
- Нелогичность;
- Отрывочность;
- Разрозненность;
- Поддержание общения одновременно с несколькими собеседниками.

Ключевой вопрос: Как бороться с клиповым мышлением?

Внимание!

Основной причиной развития клипового мышления у детей и подростков является особенность преподнесения информации в Интернете. Информация в сети подается отрывочно, в виде коротких статей или видео. Ярким примером является чтение новостей «по заголовкам». В таком случае человек менее склонен сомневаться в информации и перепроверять ее.

Считается, что клиповое мышление преобладает у тех, кто большую часть свободного времени проводит в Интернете ввиду специфики подачи информации. В среднем, современные подростки в возрасте от 12 до 17 лет тратят на Интернет почти 6 часов в день (по данным Mediascope).

У современной молодежи по данным экспертов зафиксированы проблемы, связанные с чтением. При попытке прочитать и усвоить сложный текст, (например, инструкцию), многие подростки начинают испытывать резь в глазах и головную боль.

Что способствует формированию клипового мышления:

- Музыкальные клипы;
- Реклама на ТВ;
- Электронные СМИ;
- Мобильные средства связи;
- Социальные сети и мессенджеры, такие как TikTok, YouTube.

Развитие клипового мышления проводит к следующим проблемам:

- Внушаемость;
- Плохая обучаемость;
- Гиперактивность;
- Дефицит внимания;
- Предпочтение визуальных символов логике и углублению в текст;
- Неспособность к восприятию однородной информации (в т.ч. книжного текста);
- Снижение уровня грамотности у подростков и студентов;
- Вместо логических связей выстраиваются эмоциональные;
- Ослабляется или нивелируется чувство сопереживания, а также ответственности.

Полезные советы

- Контролируйте экранное время ребенка.
- Воспользуйтесь приложениями для тренировки памяти и внимания.

Личный пример

Организуйте «время без гаджетов» - по вечерам или по выходным дням, когда не только ребенок, но и вся семья сможет максимально отвлечься от телефонов, компьютера и Интернета.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

Лига безопасного интернета

Сайт ligainternet.ru

МАНИПУЛЯЦИИ В ИНТЕРНЕТЕ: ФЕЙКИ, ЛОЖЬ, НЕДОСТОВЕРНАЯ ИНФОРМАЦИЯ

Что такое «фейк»?

Проблема верифицированных источников информации сейчас стоит очень остро не только в России, но и во всем мире. Фейк – целенаправленно распространяемая ложная информация под видом достоверной. Может выражаться в самых разных формах, таких как: текстовые материалы, новостные статьи, аудио- и видеозаписи, передачи, а иногда и целые фильмы, снятые в документальном или псевдодокументальном жанре.

Ключевой вопрос:
Жизнь в век дезинформации.
Фейки и ложь в сети

Основным местом концентрации фейков является Интернет. Подобные материалы чаще всего распространяются через интернет-мессенджеры, а уже оттуда попадают в социальные сети или «желтые» средства массовой информации.

Фейки могут распространяться с самыми разными целями:

1. Ради шутки или создания повышенного внимания какому-либо событию.
2. Для увеличения посещаемости сайта («накручивания счетчика просмотров»). Создаются «громкие» заголовки-приманки, кликнув на который пользователи переходят на сайт и таким образом увеличивают трафик этого сайта.
3. С целью дезинформации читателей о реальной ситуации: изменения настроения в обществе, отношения людей к какому-либо вопросу, создания паники или волнения среди людей.

Внимание!

Самый распространенный формат фейков, с которым сталкивался практически каждый – **фейковые новости.** Миллионы людей, подвергаясь регулярному воздействию фейков, начинают верить ложной информации, что в перспективе приводит к негативным последствиям. Лишь 49% россиян, согласно опросу, проведенному ВЦИОМ, уверены, что смогут отличить фейк от настоящей новости.

С фейками в интернете сталкиваются не только взрослые, но и дети. Ребенок может увидеть заголовок на сайте, содержащий ложную информацию. Фейки могут целенаправленно рассылаться пользователям в мессенджерах или соцсетях. Кроме того, иногда происходят взломы официальных сайтов или страниц известных организаций. В таком случае злоумышленники могут рассылать ложную информацию от их лица.

Как правило, в информационном пространстве **фейки живут относительно недолго – 3-4 дня.** Для искусственного поддержания интереса к подобному материалу совершаются «вбросы» – ложная информация поступает в Интернет через специальные каналы, откуда распространяется в настоящие СМИ, либо же расходится по пользователям и распространяется с помощью пересылки друг другу.

Кроме фейков существуют и самые настоящие «ментальные вирусы». Ментальные вирусы – это какие-либо тексты, статьи или новости, а иногда аудио- или видеозаписи, содержащие в себе определенную идею. Как и настоящие вирусы, они способны заражать сознание людей и целого общества, внедряя вредную, опасную и разрушительную идею.

Источники опасности:

- **У каждого фейка есть конкретная цель** – могут провоцировать людей на совершение опрометчивых поступков.
- **С учетом специфики Интернета - очень большой охват аудитории, скорость распространения.**
- **Могут представлять угрозу жизни и здоровью людей.**
- **Инструмент манипуляции.** Создатели фейка могут управлять подвергнувшимся воздействию как организованной структурой.

Как распознать фейк?

1. Сообщение быстро распространяется в соцсетях или мессенджерах.
2. Сообщение очень эмоциональное, вместе с тем не содержит факты, которые возможно перепроверить.
3. Передаются сведения об угрозе жизни и здоровья большого числа людей, а также о наличии многочисленных жертв.
4. Присутствует указание на то, что власти скрывают информацию во избежание паники или волнений. Именно поэтому вы не найдете ничего в СМИ. Подчеркивается, что значимая для общества информация специально утаивается.
5. Присутствует просьба о максимальном распространении информации, либо о сокрытии (ведь автор сообщил ее вам «по секрету»).
6. Присутствует указание на лицо, сообщившее новость (врач больницы, водитель скорой, учитель школы, знакомый знакомого), либо информация о месте, где что-то произошло (номер больницы, название города, адрес школы).
7. Источник информации сложно установить.

При проверке информации есть ряд маркеров, на которые очень важно обратить внимание:

1. **Оригинал всегда лучше любого пересказа,** поэтому всегда важно искать оригинальный источник информации и задумываться на сколько этому источнику информации можно доверять. Не является ли, например, источником новости желтое СМИ или какая-то из «тизерных» сеток, которые занимаются привлечением трафика пользователей с помощью «кликбейтных», то есть громких заголовков.
2. **При работе с оригинальными источниками важно смотреть взаимосвязь между этими источниками информации.** Если информация опубликована в разных источниках, то как они сами между собой связаны. Не является ли это партнерской сетью ресурсов или единой сетью распространения информации.
3. **Чаще всего разнообразие фейковых сообщений очень низкое,** постоянно публикуется фактически одно и то же сообщение. Практически все фейки являются перепостами.
4. **При сравнении оригинальной настоящей новости и фейка, у настоящей новости всегда очень много свидетелей,** очень много участников, они по-разному рассказывают своими словами о том, что произошло. Настоящая новость имеет очень много серьезных верифицированных источников информации. Сейчас ни одна заслуживающая внимания новость не проходит мимо ведущих средств массовой информации.
5. **Очень важно обратить внимание на контекст новости** и проверять полную суть любой цитаты, которая используется в том или ином сообщении. Не стоит доверять ссылкам на громкие и авторитетные имена. Проверять нужно как цитаты, так и факты, кому бы они не принадлежали, какая бы известная фамилия ни была озвучена.
6. **Очень важно обращать внимание на суть, смысл самого материала,** а не на мелкие детали, которых очень много в фейках. Они, таким образом, отвлекают внимание от содержания, придавая некую достоверность материалу.
7. **В новой информационной реальности важно научиться доверять серьезным средствам массовой информации, официальным источникам,** которые дорожат своей репутацией и ответственно относятся к распространению новых сведений и данных.

Полезные советы

Если вы получили или обнаружили недостоверную информацию, есть простые шаги, с помощью которых можно защитить себя, своих друзей и родственников от массового распространения этого сообщения:

1. **Стоит дождаться официального подтверждения или опровержения** громкой новости, прежде чем пересылать что-то друзьям и знакомым.
2. **Обратитесь в службу поддержки** и направьте туда все имеющиеся у вас ссылки, скриншоты и т.д.
3. **Обратитесь в полицию, Роскомнадзор** и прикрепите ссылки и скриншоты страниц, содержащих недостоверную информацию.
4. **Если вы считаете, что сообщение или публикация является общественно опасной, вы можете прислать скриншот и ссылку в Лигу безопасного Интернета по адресу: info@ligainternet.ru или в сообщениях VK: vk.com/liga.**

Внимание!

В случае обнаружения фейковой информации не стесняйтесь и пользуйтесь кнопкой «Пожаловаться» (в случае с социальными сетями или мессенджерами). Мессенджеры и соцсети должны оперативно блокировать такие сообщения и публикации.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

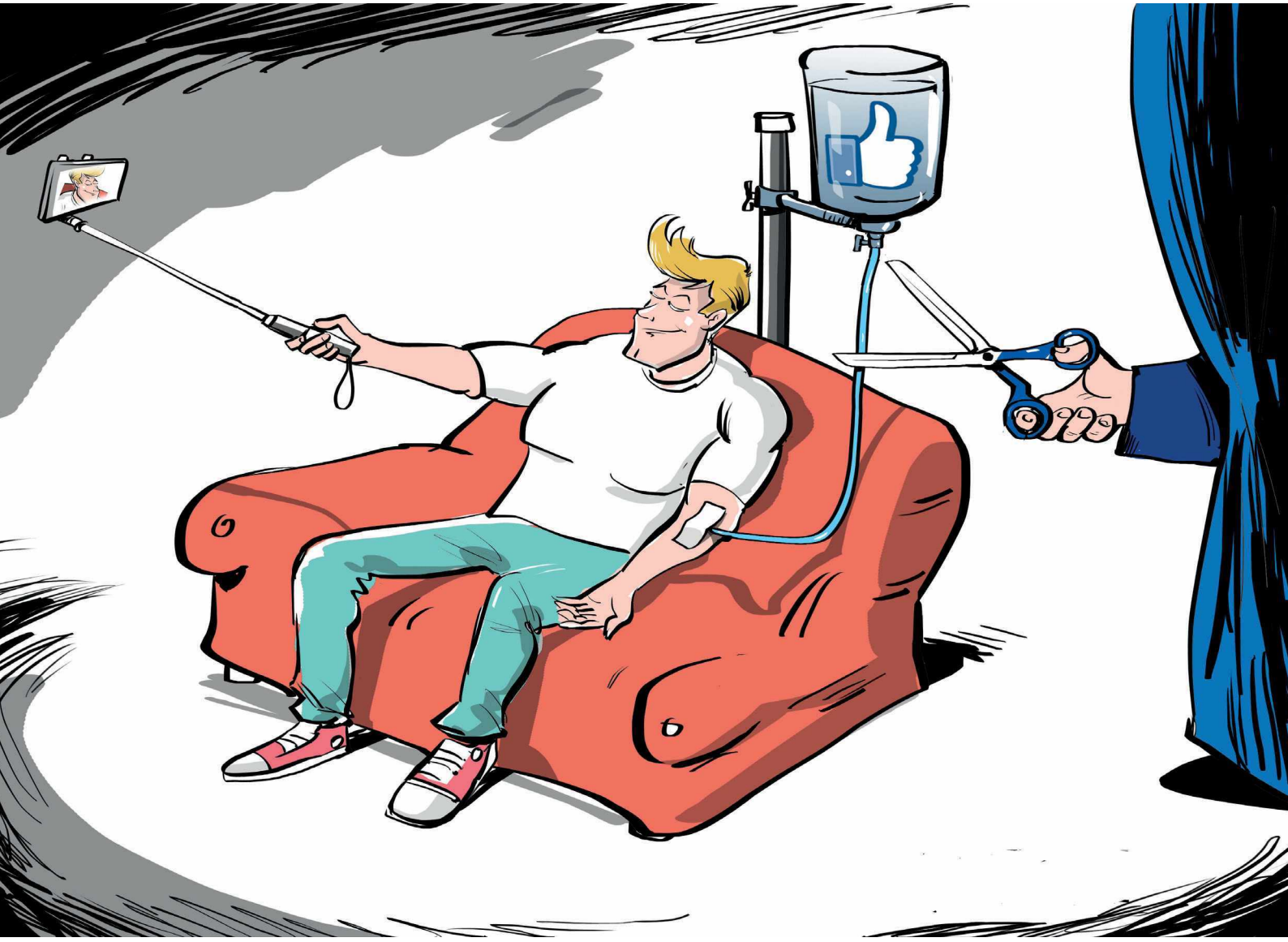
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Сайт ligainternet.ru

ВОЗДЕЙСТВИЕ ВИРТУАЛЬНОЙ ЖИЗНИ: ИЛЛЮЗИИ СОЦСЕТЕЙ

«Мультиреальность» как ценность и проблема

Современные дети и взрослые существуют одновременно в двух реальностях – реальной и виртуальной. Перенос частной жизни в виртуальное пространство приводит к тому, что цифровой мир не просто дополняет реальную жизнь, а становится ее полноценной частью. Это называют «мультиреальностью».



Ключевой вопрос

Какие существуют проблемы в «мультиреальности», как их минимизировать?

Внимание!

Виртуальная жизнь может целиком заменить реальную, люди пытаются переносить шаблоны и модели подведения из виртуального мира в реальный.

Признаки чрезмерного погружения человека в виртуальный мир:

- Если во время разговора или дискуссии в реальной жизни человек не может отстоять свою точку зрения, он попытается «забанить» (заблокировать) собеседника так, как сделал бы это в соцсети – уйти от разговора, перестать отвечать, игнорировать собеседника.

- Многие дети сегодня учатся пользоваться смартфонами и Интернетом еще до того, как научатся писать и читать. С самого раннего возраста они начинают поглощать огромное количество не самого качественного развлекательного контента. Каждый четвертый ребенок в возрасте от 0 до 12 месяцев использует Интернет. Более половины детей в возрасте до 3 лет используют Интернет каждый день. Это приводит к изменению умственного развития, ухудшению памяти и социальных навыков.

- Происходящее в социальных сетях представляет для детей больший интерес, чем собственные впечатлений в реальной жизни. Всё интересное, что происходит в жизни, необходимо фотографировать и выкладывать в соцсети. Например, достопримечательность на отдыхе необходимо сфотографировать и «запостить» в соцсети. Публикация для пользователя гораздо важнее, чем сама достопримечательность.

Преодолевайте иллюзии! Соцсети постоянно создают иллюзии, которым подвержено большинство пользователей. Эти иллюзии часто переносятся и в реальный мир:

Иллюзия недолговечности – большинство пользователей уверено, что все, что они выложили в сеть, будет жить несколько часов или дней. Но старые публикации никуда не пропадают, даже если их удалить. Они хранятся и формируют обширный цифровой след об авторе, их можно восстановить и использовать для шантажа или компромата. По данным Лаборатории Касперского, 22% детей выкладывали в Интернет информацию, о размещении которой в последствии жалели.

Иллюзия доброжелательности – авторы публикаций в социальных сетях ожидают видеть похвалу и одобрение в свой адрес. Несогласных или возмущенных людей можно просто «забанить», так они не смогут комментировать и даже просматривать публикации пользователя. Чем больше пользователь находится в плену этой иллюзии, тем меньше он готов к нападениям недоброжелателей и «троллей» в соцсети и тем сильнее будет травмирован в случае травли или агрессии. 30% детей, по данным Лаборатории Касперского, близко знакомы с травлей в социальных сетях – они либо сами были ей подвержены, либо становились очевидцами подобного.

Иллюзия ценности – многие пользователи уверены, что все, что они пишут и публикуют – нужно и полезно для остальных пользователей. В какой-то степени, это действительно так. Только вся эта информация нужна и полезна не для других пользователей, а для самой соцсети и ее разработчиков. Ведь чем больше информации о себе вы опубликуете, тем более точный портрет смогут собрать о вас алгоритмы соцсетей и тем более дорогую рекламу смогут вам показывать.

Полезные советы:

- **Не переносите поведение из социальных сетей в реальный мир!** Общение с собеседником лично совершенно не похоже на общение в чате.
- **Внимательно относитесь к тому, что публикуете!** Если вы не готовы столкнуться с критикой – лучше не публиковать. В Интернете много недоброжелателей.
- **Помните,** что любая информация в Интернете, фото, видео или сообщения могут быть восстановлены даже спустя много лет после удаления.
- **Общайтесь с людьми в реальности,** а не в социальных сетях. Чем меньше вы пользуетесь смартфоном, тем лучше!

Личный пример

Отключайте смартфон хотя бы на несколько часов в день. Цените время, которое вы проводите вместе с семьей, не тратьте его на социальные сети и приложения.

По данным исследования ВЦИОМ *(Всероссийский центр изучения общественного мнения)* **почти каждый третий (29%) пользователь соцсетей и мессенджеров в России тратит на них более 3 часов в день, а среди молодежи 18-24 лет эта цифра достигает 72%.**

По данным Лаборатории Касперского:

22% детей жалели
о том, что выкладывали в Интернет.

30% детей сталкивались с травлей в соцсетях –
подвергались ей либо видели травлю в отношении других.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru