

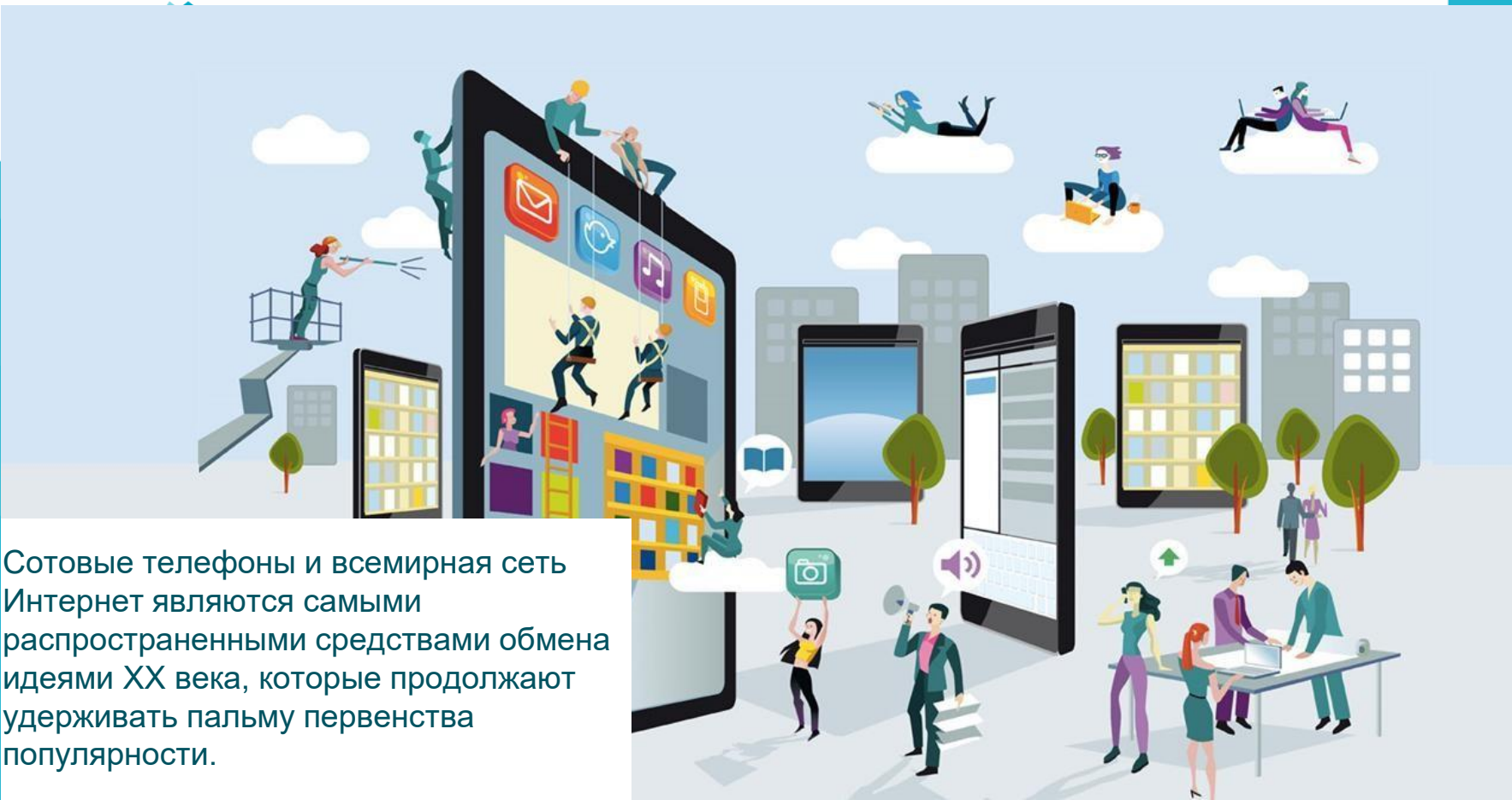


РГППУ
Российский государственный
профессионально-педагогический
университет

Безопасность в сети Интернет



Ломовцева Наталья Викторовна
К.п.н., доцент кафедры Информационных систем и
технологий



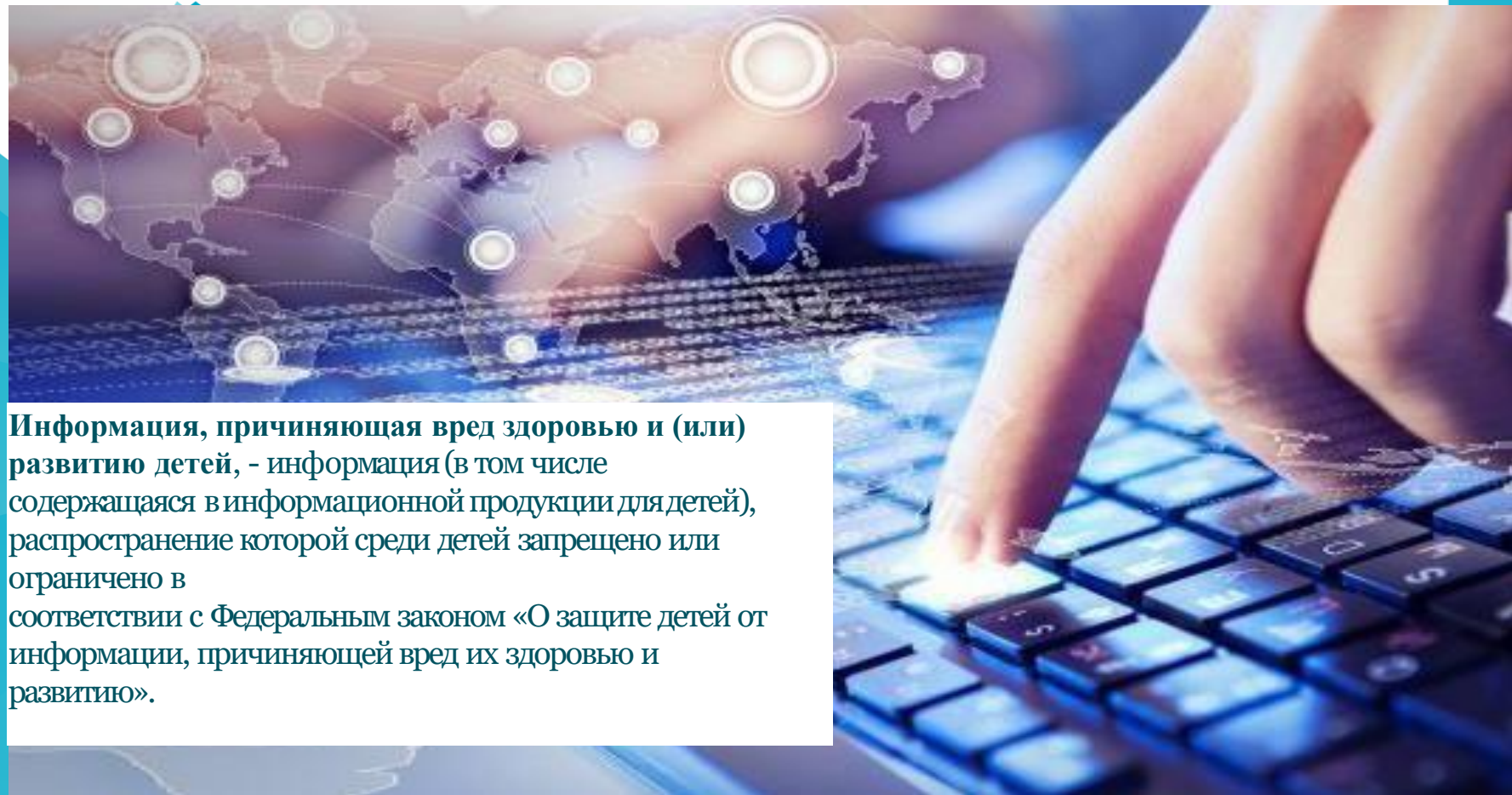
Сотовые телефоны и всемирная сеть Интернет являются самыми распространенными средствами обмена идеями XX века, которые продолжают удерживать пальму первенства популярности.

Нормативно - правовая база обеспечения безопасности детей и подростков в сети Интернет

1. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в РФ», ст. 4, 37 Закона РФ от 27.12.1991 «О средствах массовой информации» № 2124-1.
2. Стратегия национальной безопасности РФ до 2020 года, утвержденной Указом Президента РФ от 12.05.2009 № 537.
3. Доктрина информационной безопасности РФ, утверждена Президентом РФ 09.09.2000 № ПР-1895.
4. Письмо Министерства образования и науки Российской Федерации от 10.11.2006 № АС-1299/03 «О реализации контентной фильтрации доступа образовательных учреждений, подключаемых к сети Интернет в рамках приоритетного национального проекта «Образование».
- 5.
6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».



Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правила медиабезопасности детей при распространении на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях радиотелефонной связи. Закон содержит ряд инновационных норм, предусматривающих создание организационно-правовых механизмов защиты детей от распространения в сети Интернет вредной для них информации.



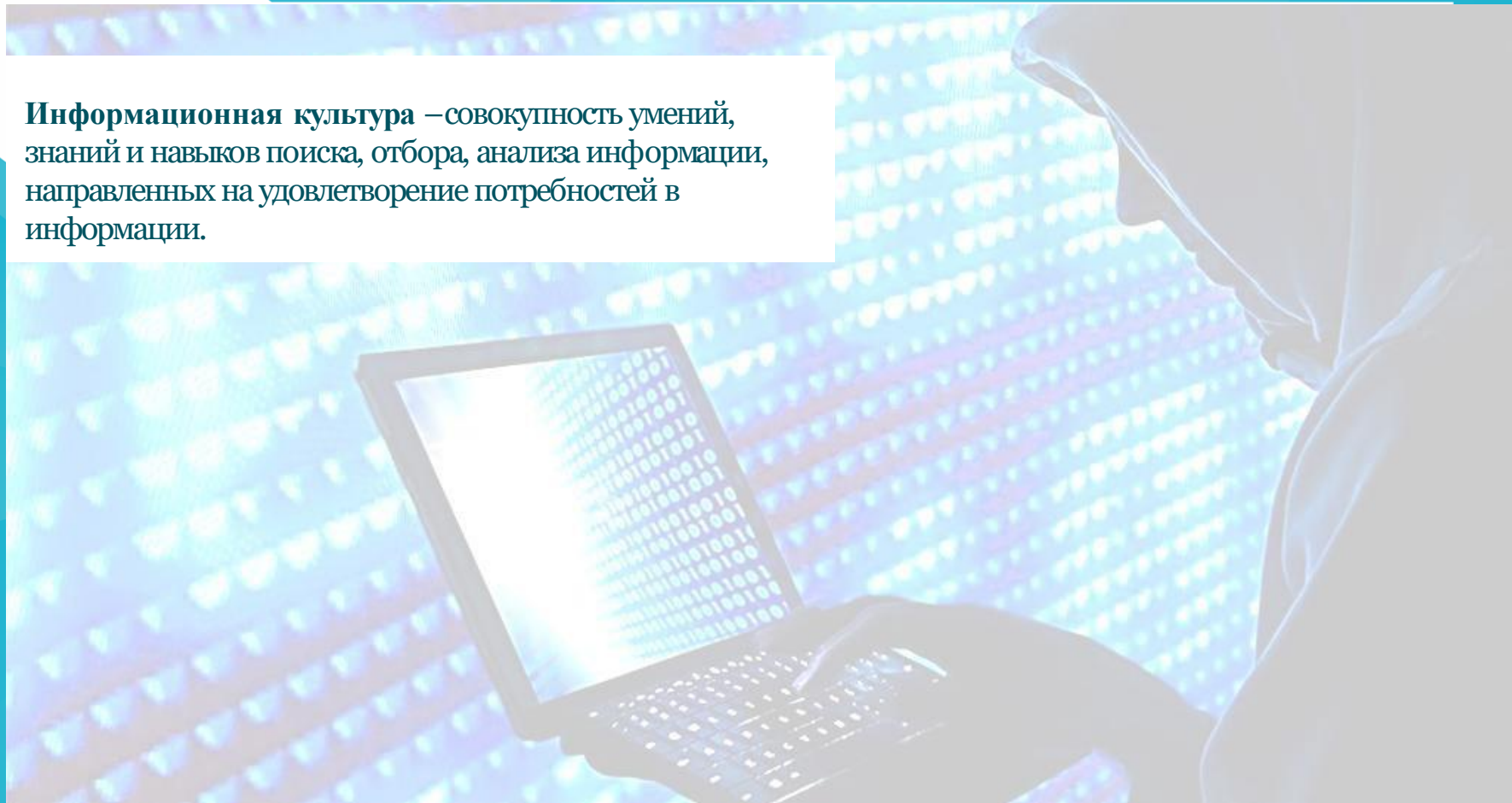
Информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию».

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»

Статья 5. Информация, запрещенная для распространения среди детей

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, призывающая принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи
- оправдывающая противоправное поведение
- содержащая нецензурную брань
- содержащая информацию порнографического характера

Информационная культура – совокупность умений, знаний и навыков поиска, отбора, анализа информации, направленных на удовлетворение потребностей в информации.





РГППУ
Российский государственный
профессионально-педагогический
университет

Риски, связанные с использованием интернета детьми и подростками

Контентные риски

*Коммуникационные
риски*

*Электронные (кибер)
риски*

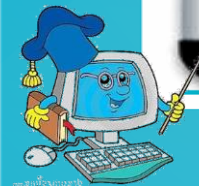
*Потребительские
риски*

*Интернет-
зависимость*

*Риски, связанные с
вовлечением
несовершеннолетних
в опасные группы и
сообщества*

Признаки подверженности несовершеннолетних интернет-рискам (интернет-зависимого поведения, участия в «опасных» группах):

- резкое изменение фона настроения и поведения, преобладание подавленного настроения;
- значительное время пребывания в Интернете, переживание тревоги, негативных эмоций при невозможности выхода в Интернет даже короткое время;
- общение в группе и просмотр видеосюжетов в ночное время, следствием чего являются трудности в пробуждении, ребенок выглядит не выспавшимся;
- сокрытие от взрослых своих страниц и действий в Интернете, нежелание ребенка обсуждать новости группы, свои действия в ней;
- ведение в сети одновременно нескольких страниц под разными именами, особенно от имени и девочки, и мальчика;
- появление в речи и на страницах в сети рисунков, афоризмов, тегов, связанных с суицидальным поведением .



РГППУ

Российский государственный
профессионально-педагогический
университет



хорошая
успеваемость

общителен

не замкнут

✓ Как понять, что ребенок
в опасности?



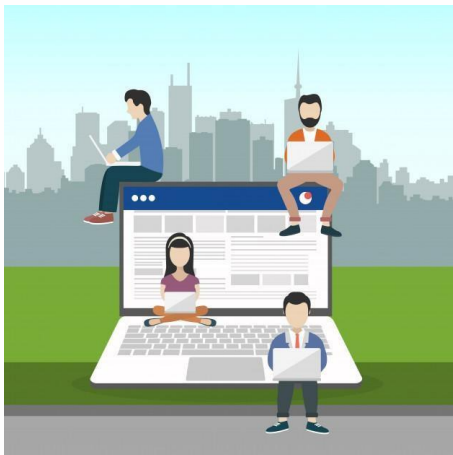
Проблемы безопасности детей в Интернете актуальны для педагогического сообщества, поскольку в учреждениях образования активно используются интернет-ресурсы.

Как защитить ребенка от интернет-рисков?



Что делать нужно сделать

Советы по интернет-безопасности



- посещайте Интернет вместе с детьми;
- объясните детям, что не следует скрывать, если в Интернете что-либо вызвало беспокойство;
- объясните ребёнку, что нельзя использовать реальное имя, помогите выбрать регистрационное имя;
- объясните ребенку, что нельзя выдавать свои личные данные;
- научите детей уважать собеседников в Интернете;
- расскажите детям, что не стоит встречаться с друзьями из Интернета;
- не забывайте контролировать детей в Интернете с помощью специального программного обеспечения.

Интернет- безопасность в семье



- 
- ✓ какие сайты могут посещать дети и что им разрешается там делать;
 - ✓ сколько времени дети могут проводить в Интернете;
 - ✓ что делать, если что-либо вызывает у детей ощущение дискомфорта;
 - ✓ как защитить личные данные;
 - ✓ как следить за безопасностью;
 - ✓ как вести себя при общении;
 - ✓ как пользоваться службами чатов, группами новостей и мгновенными сообщениями.

Интернет- безопасность в семье



Интернет- безопасность в семье



Программа «Родительский контроль»
позволяет:

- ✓ сформировать списки контактов, переписка с которыми будет разрешена или запрещена;
- ✓ задать ключевые слова, наличие которых будет проверяться в сообщениях;
- ✓ указать личную информацию, пересылка которой будет запрещена.

Профилактическая работа педагога ведется в двух направлениях:

1. Обогащение развивающего ресурса образовательной среды за счет повышения психолого- педагогической компетентности педагогов и родителей через информирование и включение в разработку и реализацию профилактических программ, в совместную с несовершеннолетними активную профилактическую работу.
2. Формирование ресурсов устойчивости к рискам у несовершеннолетних за счет развития их личностных качеств, поведенческих стратегий через активное социально-психологическое обучение и педагогическое воздействие.

Устойчивость к интернет-рискам и угрозам предполагает: формирование основ осведомленности школьников об особенностях распространения информации в Сети, включая невозможность контролировать ее достоверность и т.д.;

- ❖ формирование личностных качеств школьников, связанных со способностью брать на себя ответственность, готовностью к сознательному выбору социальных ориентиров и организации в соответствии с ними своей деятельности: социальной сензитивности, эмпатии, рефлексивность, чувство социальной уверенности.
- ❖ развитие социальной умелости: навыков безопасной самопрезентации и взаимодействия с другими людьми в сети Интернет, умений вступать в контакт и выходить из контакта,
- ❖ адекватно выражать свои чувства, переживания; твердо и без агрессии реагировать на мнение и оценки другого;
- ❖ критически анализировать информацию и содержание сообщений, особенно сообщений, призывающих к каким либо действиям;
- ❖ умений ставить цели и планировать свои действия, соотносить призывы со своими целями и планами; умений выдвигать альтернативные способы действий, говорить «нет», запрашивать помощь, преодолевать трудности, разрешать конфликты и межличностные проблемы.

Первое направление реализуется по следующему алгоритму:

1. **Этап.** Информирование педагогов и родителей об интернет-рисках и угрозах, психологических механизмах их распространения, о средствах и способах защиты, о психологических ресурсах устойчивости к воздействию рисков и угроз, задачах по их развитию, условиях и средствах развития;
2. **Этап.** Привлечение педагогов и родителей к анализу своих возможностей по управлению интернет-рисками, а также созданных в семье и образовательной организации условий для развития устойчивости несовершеннолетних к интернет-рискам и угрозам;
3. **Этап.** Выработка условий развития ресурсов устойчивости несовершеннолетних к интернет-рискам и угрозам в образовательной организации и семье;
4. **Этап.** Разработка и реализация совместно с педагогами психолого-педагогических программ развития устойчивости несовершеннолетних к интернет-рискам и угрозам;
5. **Этап.** Вовлечение педагогов и родителей в активную, совместную с несовершеннолетними профилактическую работу, в создание позитивно ориентированной развивающей интернет-среды, представляющей несовершеннолетним возможности для самореализации;
6. **Этап.** (Дополнительный) . Консультирование по запросу по проблемам защиты несовершеннолетних от интернет-рисков и угроз.
7. **Этап.** Рефлексивно-аналитический: привлечение педагогов и родителей к анализу эффективности профилактической работы.

Реализация второго направления предусматривает следующие этапы:

- 1.Этап.** Изучение информированности несовершеннолетних об интернет-рисках и угрозах, средствах и способах защиты от них;
- 2.Этап.** Информирование несовершеннолетних о средствах и способах защиты от интернет-рисков и угроз (с учетом данных, полученных на 1 этапе), о правилах работы в Сети, о ресурсах устойчивости к интернет-угрозам, способах их развития;
- 3.Этап.** Организация эмоционально насыщенных профилактических мероприятий для несовершеннолетних с учетом возрастных особенностей (по параллелям или ступеням обучения);
- 4.Этап.** Проведение совместно с педагогами занятий по психолого-педагогическим программам развития ресурсов устойчивости к интернет-рискам и угрозам на уроках и во внеурочной деятельности.
- 5.Этап.** Вовлечение несовершеннолетних в совместную с педагогами и родителями профилактическую работу, в создание и модерирование позитивно ориентированной развивающей интернет-среды, обеспечивающей самореализацию.
- 6.Этап.** (Дополнительный). Организация индивидуальной или групповой диагностико-коррекционной работы по запросу классных руководителей, родителей, несовершеннолетних, направленной на выявление групп риска (могут быть использованы данные, полученные на 1 этапе или диагностика склонности к интернет-зависимости), на развитие ресурсов устойчивости к рискам и угрозам.
- 7.Этап.** Рефлексивно-аналитический: привлечение несовершеннолетних к анализу привлекательности и результативности профилактической работы.

интересуйтесь реальной и
виртуальной жизнью детей

любите детей

прощайте ребёнка,
хвалите,
содействуйте

поддерживайте и
подбадривайте ребенка

учитесь слушать и слышать
ребёнка

станьте для ребёнка другом

будьте в контакте с детьми



**ОБЩЕНИЕ
ВЗРОСЛЫХ С ДЕТЬМИ**



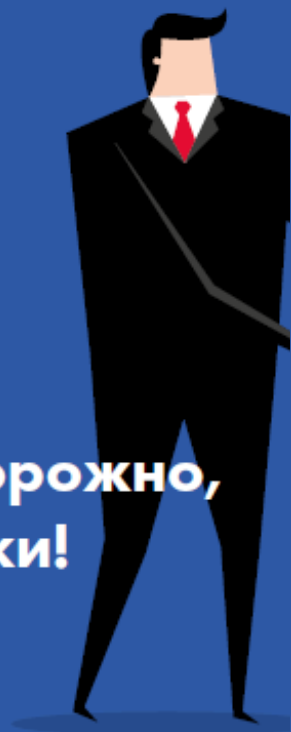
Медиабезопасность детей в сети Интернет должна обеспечиваться совместными усилиями школы и родителей. В школе может быть разработана программа по медиабезопасности, которая включает в себя уроки и внеклассные мероприятия по медиабезопасности, неделю медиабезопасности, тематические модули по медиабезопасности в рамках предметов технология или информатика, мероприятия по медиабезопасности для родителей.



Никакого
везения,
ТОЛЬКО
опасения

История #1





ВИДЫ ФЕЙКОВ:



Фейковые страницы

Страницы, на которых размещена ложная информация о владельце



Фейковые конкурсы

Конкурсы, в которых заведомо невозможно выиграть



Фейковые отзывы

Отзывы, написанные с помощью ботов или фейковых страниц и сообщающие недостоверную информацию о чем-либо

**Осторожно,
фейки!**

ФЕЙК — ЧТО-ТО ЛОЖ
НЕНАСТОЯЩЕЕ, СОЗД
ОБМАНУТЬ ТЕБЯ. В ИН
ВСТРЕЧАЮТСЯ НА КА

Фейковые страницы

КАКИЕ ОНИ БЫВАЮТ?

- Пустые страницы – боты, которые накручивают статистику за деньги.
- Страницы, дублирующие информацию и фотографии со страниц разных людей (актеров, музыкантов и т.д.)

ЧТО ОНИ МОГУТ?

- Сбирать твою информацию и продавать ее неизвестно кому
- Быть прикрытием для преступников и мошенников
- Оставлять неприятные комментарии на твоей странице
- Предлагать тебе участие в фейковых конкурсах
- Вымогать у тебя деньги

КАК ПОНЯТЬ, ЧТО СТРАНИЦА – ФЕЙК?

1. Личная информация либо не заполнена, либо заполнена по минимуму
2. Аватарки либо нет, либо на аватарке не фотография человека, а картинка из интернета
3. Друзей совсем нет или очень мало
4. Фотографии выложены в один день, либо с разницей в несколько дней.



Написать сообщение



Михаил Молонин

1

online

Хроника жизни

Дата рождения:

15 декабря 1980 г.

Город:

Москва

10 друзей

5 подписчиков

24 фотографии

Фотография Михаила 24

4

показать на карте



ФЕЙКОВЫЕ КОНКУРСЫ



Для чего они проводятся?

- Бесплатная накрутка подписчиков — люди вступают в группу, потому что это обязательное условие для победы, потом конкурс либо не проводится вообще, либо призы достаются друзьям администраторов.
- Обман на деньги — проводится конкурс, у победителей под разными предлогами просят деньги, но призы не отдают.



Как понять, что конкурс фейковый?

- В правилах написано, что победитель оплачивает доставку приза.
- Участие в конкурсе платное.
- Подписчики лишут в комментариях, что организаторам нельзя доверять.
- Администраторы не публикуют видео или трансляцию с выбором победителей.

А если конкурс не фейковый и я в хочу в нем участвовать?

- Внимательно читай правила конкурса перед участием (обычно полный перечень правил находится на прикрепленной wiki-странице или в осуждении).
- Прочитай комментарии к записям о старых конкурсах группы/сообщества. Убедись, что они не фейковые.
- Не участвуй больше, чем в 2-3 конкурсах сразу. Удаляй старые репосты.

ФЕЙКОВЫЕ ОТЗЫВЫ

Для чего их пишут?

- Чтобы продать некачественный товар
- Чтобы обмануть и не продать вообще ничего
- Чтобы испортить репутацию

Как понять, что отзывы ненастоящие?



 22.05.2018 Круто! Я в восторге!	Не содержит личного мнения, ограничиваются словами «Вау! Круто! Я в восторге!»
 29.05.2018 Ужасно! Сдали в ремонт через неделю после покупки!	Не содержит подробного описания сложившейся проблемы и причин негативного отношения.
 22.05.2018 Отлично!	Размещены в один день.
 22.05.2018 У данной модели высокое качество	Размещены в один день.
 28.05.2018 По промокоду OTZIV123 вы получите скидку!	Похожи на рекламу
 22.05.2018 Спасибо за быструю доставку!	Имеют фактические ошибки (например, хавают доставку, а доставки на сайте нет)

Что выделяет фейковые отзывы.

1. В один день написано большое количество отзывов
2. В отзыве есть слова в превосходной степени
3. Пользователь пишет много отзывов в один день
4. В отзыве указаны имена нескольких сотрудников компании
5. Фото из отзыва используется в других отзывах
6. Рекламные, обезличенные или общие формулировки
7. Отзыв написан спустя несколько лет после покупки
8. Грубые ошибки в отзыве
9. В отзыве оправдывается недостаток товара



Жизнь
напоказ:
**ошибки
в Сети —
потери
в реале**



История #2

Общие правила безопасности в Instagram



Не публикуй геометку своего дома



Не выкладывай в сеть фотографии, по которым незнакомый человек может понять, в какой квартире ты живешь (фотографии из окна, фотографии дома и номера квартиры)



Сделай свой профиль закрытым, чтобы твои фотографии и stories могли смотреть только люди, которым ты доверяешь

Советы по безопасности:

1. Выберите **НАДЕЖНЫЙ** пароль. Используйте комбинацию по крайней мере из 6 цифр, букв и символов (например, ! или &). Пароль не должен использоваться на других сайтах.
2. Регулярно **МЕНЯЙТЕ** пароль, особенно если получите от Instagram сообщение с просьбой это сделать.
3. Включите **ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ** в качестве дополнительной меры безопасности.
4. Убедитесь в безопасности своего аккаунта **ЭЛЕКТРОННОЙ ПОЧТЫ**.
5. Выходите из аккаунта Instagram, если используете компьютер или телефон, которым пользуются другие люди. **НЕ УСТАНАВЛИВАЙТЕ ФЛАЖОК** "Запомнить меня", если входите в систему с общедоступного компьютера.
6. Будьте особо **ВНИМАТЕЛЬНЫ**, предоставляя сторонним приложениям доступ к своему аккаунту.

Если
ты чего-то
не видишь,
не значит,
что этого не
существует

Знаешь ли ты, что
твои фотографии
хранят намного
больше информации,
чем на первый
взгляд?



До настройки:

1. На какое устройство она снята?
2. При каких настройках она снята?
3. Координаты
4. Дата и время
5. Размер и формат файла
6. В какой операционной системе редактировались фотографии?

Все это называется **мета-данные** или **exif-данные**. К счастью, социальные сети научились удалять лишнюю информацию с фотографий. Но ты можешь сделать это сам, воспользовавшись любой программой для удаления мета-данных с фотографий.



После настройки:

1. Время и дата
2. Размер и формат файла

Для этого подойдут следующие программы и сервисы:

MAC/PC — Easy Exif Delete, Exif Pilot PRO, iOS — Exif Viewer, Android — Photo Exif Editor, онлайн-сервис IMGonline.



И еще несколько
простых советов:

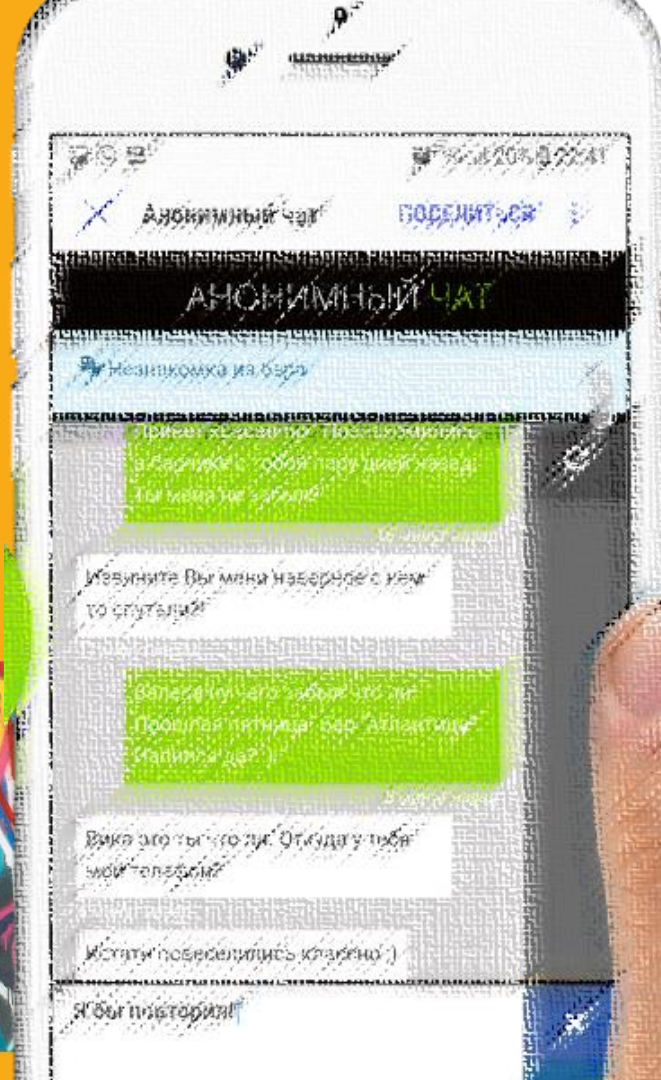
- Запрети приложению «Камера» на телефоне доступ к геолокации
- Вставляй геолокацию в социальных сетях вручную
- Не загружай фотографии

От хейтеров
до хайпов!

Гид по социальным
сетям



Любовь
зла: **как**
социальные
сети
разбивают
сердца



История #3



1. Пиши в Сети только то, что можешь сказать, глядя в глаза в реальном мире.

2. Не показывай информацию о себе никому, кроме близких друзей.

3. Не травь других. Если травят тебя — закрывай аккаунт.

4. Не отвечай на спам.

5. Не открывай файлы, которые прислали неизвестные тебе люди.

6. Встречайся с новыми друзьями из виртуального мира только днем и в многолюдных местах.

7. Помни — виртуальные знакомые могут быть не теми, за кого себя выдают.

1. Пиши в Сети только то, что можешь сказать, глядя в глаза в реальном мире.
2. Не показывай информацию о себе никому, кроме близких друзей.
3. Не травь других. Если травят тебя — закрывай аккаунт.
4. Не отвечай на спам.
5. Не открывай файлы, которые прислали неизвестные тебе люди.
6. Встречайся с новыми друзьями из виртуального мира только днем и в многолюдных местах.
7. Помни — виртуальные знакомые могут быть не теми, за кого себя выдают.

Остерегайся травли!

Травля — агрессивные действия в адрес человека, имеющие цель причинить ему вред.

Виды травли



Оскорбление



Преследование



Запугивание



Распространение
слухов



Распространение
откровенных
фото

Миссия
«Пойти на
концерт»
провалена



История #4

Какую информацию нельзя выкладывать в сеть и почему?



1. Фотографии авиабилетов
2. Фотографии паспорта или других документов в открытом виде
3. Фотографии билетов на выставки, концерты, фестивали и в музеи
4. Номер телефона
5. Пароли
6. Домашний адрес

ПОЛЕЗНЫЕ ССЫЛКИ И РЕСУРСЫ

Полезные ресурсы:

- Телефон доверия для детей, подростков и родителей: <http://telefon-doveria.ru/>
- Дети России ОНЛАЙН: <http://detionline.com/>
- Я - родитель: <http://www.ya-roditel.ru/>
- Фонд поддержки детей, находящихся в трудной жизненной ситуации: <http://fond-detyam.ru/>
- Информационный портал о всех видах зависимостей, связанных с компьютерными и мобильными устройствами: <http://netaddiction.ru>
- Всероссийский семинар «Профилактика суицидального поведения детей и подростков, связанного с влиянием сети Интернет»: <http://www.fcprc.ru/training/webinars/12-17/program>
- Типовые сценарии педагогического совета и родительского собрания: «Профилактика интернет-рисков и угроз жизни детей и подростков», Федеральное государственное бюджетное научное учреждение «Центр защиты прав и интересов детей»: <http://fcprc.ru/news/profilaktika-internetriskovi-ugroz-zhizni-detej-i-podrostkov>

ПОЛЕЗНЫЕ ССЫЛКИ И РЕСУРСЫ

Полезные ресурсы:

- Информационно-аналитический журнал «Дети в информационном обществе» (в рамках Года безопасного Интернета в России): <http://www.fid.su/projects/journal>**
- Специализированные страницы сайта ФГБНУ «Центр защиты прав и интересов детей»: «ПОДДЕРЖКА ДЕТСТВА», «ТВОЕ ПРАВО», «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ», «ЦЕННОСТЬ ЖИЗНИ»: <http://www.fcprc.ru>**
- Научно-методический журнал «Образование личности»: <http://www.oljournal.ru>**
- Учебно-методический журнал «Профилактика зависимостей»: <http://профилактика-зависимостей.рф>**