

# УЧИТЕЛЯ, ДЕТИ И РОДИТЕЛИ В ЦИФРОВОМ МИРЕ



KASPERSKY®

  
ПРОСВЕЩЕНИЕ  
ИЗДАТЕЛЬСТВО



Учебное пособие «Информационная безопасность, или на расстоянии одного вируса» разработано совместными усилиями специалистов и «Издательства «Просвещение» - крупнейшего в России издательства учебной литературы

и

«Лаборатория Касперского» - международной компании, специализирующейся на разработке систем защиты от различных киберугроз

# ИНДЕКС ЦИФРОВОЙ ГРАМОТНОСТИ

цифроваяграмотность.рф



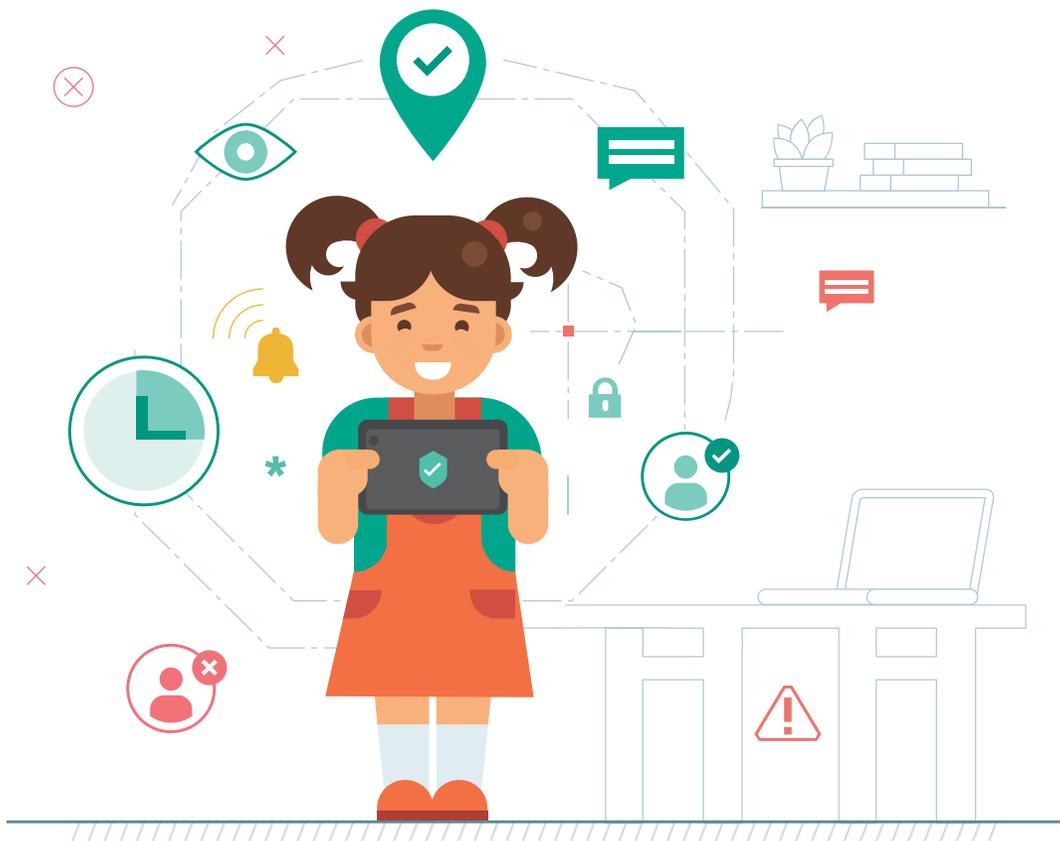
# Интернет и реальность

# ВОВЛЕЧЕННОСТЬ В ИСПОЛЬЗОВАНИЕ УСТРОЙСТВ



**85%** детей не могут обойтись без гаджетов.

В частности, **почти 70%** детей 7-14 лет говорят, что не смогут обойтись без своего смартфона. С возрастом этот показатель увеличивается и к 16-18 годам достигает **80%**.



## ПОВЕДЕНИЕ РЕБЕНКА В ИНТЕРНЕТЕ



**Почти половина** детей признается, что скрывает от своих родителей что-то из своей интернет-жизни. Чаще всего это время, которое они проводят перед экраном **и/или сайты**, на которые они заходят.

## КОМПЬЮТЕРНЫЕ ИГРЫ



Данные показывают, что **9 из 10** школьников играют в компьютерные игры.

# АКТИВНОСТЬ ДЕТЕЙ



Если рассматривать всех детей, то основными функциями интернета и гаджетов являются: **игры, общение** и **получение развлекательного контента**.  
Учеба только **на пятом месте**.



# КОНТРОЛЬ СО СТОРОНЫ РОДИТЕЛЕЙ (ОБЩАЯ ПРАКТИКА)



**Четверть** всех родителей школьников утверждает, что их дети проводят все свободное время в гаджетах/интернете. По мере взросления детей время, проводимое ими в интернете, **увеличивается**, а вот контроль со стороны родителей **ослабевает**.



Наиболее **резкий рост** количества детей, постоянно проводящих время в интернете, происходит при переходе ребенка из возрастной группы **10-12 лет** в **13-15 лет**.



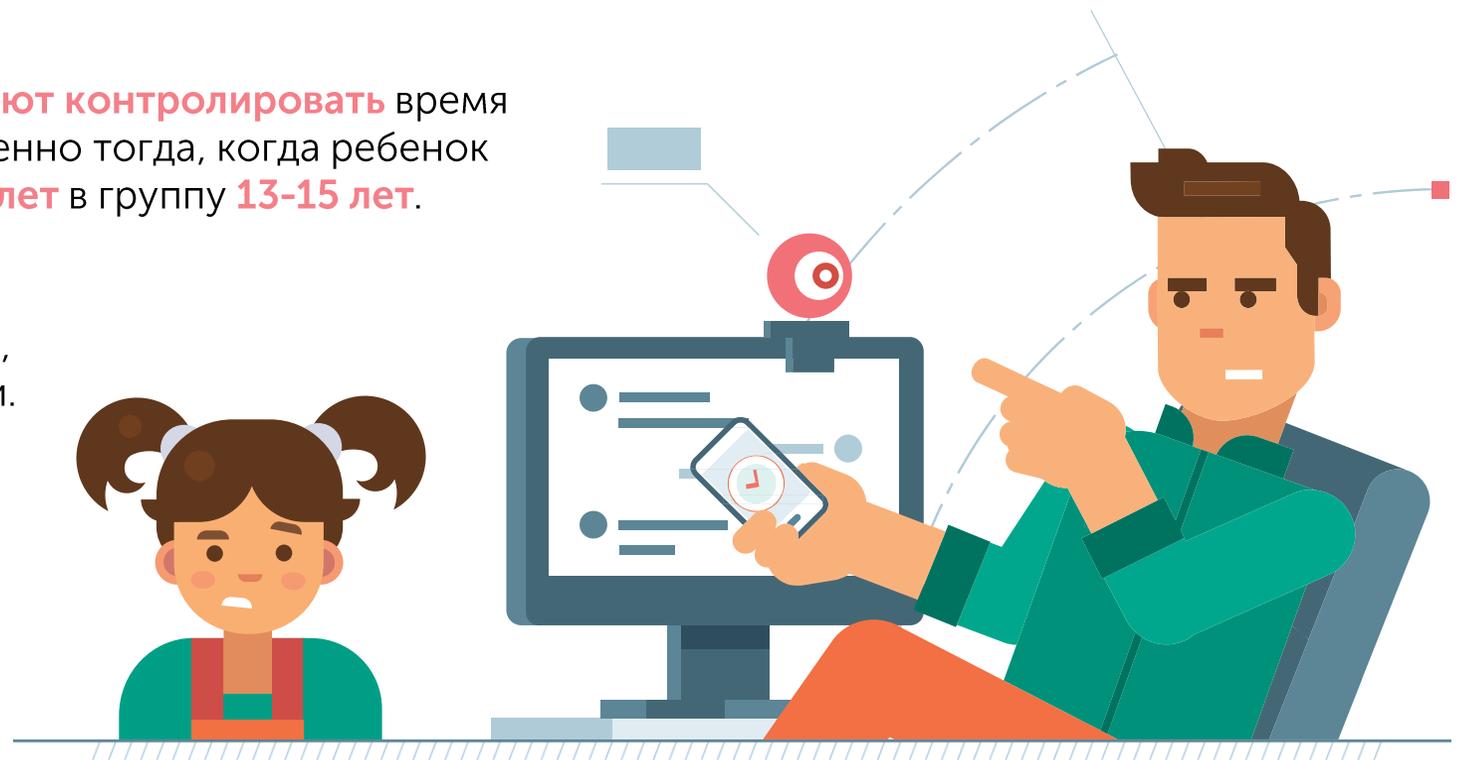
При этом чаще всего родители **перестают контролировать** время пребывания своих детей в гаджетах, именно тогда, когда ребенок переходит из возрастной группы **10-12 лет** в группу **13-15 лет**.



**35%** родителей не контролируют время, которое ребенок проводит с гаджетами.



**59%** родителей не контролируют действия своих детей в сети.



## И ИЗДАТЕЛЬСТВО ПРОСВЕЩЕНИЕ - УЧИТЕЛЯМ И ДЕТЯМ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИЛИ НА РАССТОЯНИИ ОДНОГО ВИРУСА. 7-9 КЛАССЫ

Автор – Наместникова Мария Сергеевна

Уникальный материал: создан лучшими экспертами по информационной безопасности совместно с ведущим издательством учебной литературы



# Веб серфинг

# ГДЕ ГУЛЯЮТ ДЕТИ В ИНТЕРНЕТЕ?



\*Статистика облачного сервиса Kaspersky Security Network. Посещения различных интернет-ресурсов при включенном «Родительском контроле» на ПК в России. Усредненный показатель за последние 12 месяцев.

# И ЧТО ОНИ ИЩУТ?

1	переводчик	12	одноклассники
2	ютуб	13	гугл
3	вк	14	погода
4	порно	15	картинки
5	яндекс	16	учи ру
6	секс	17	скачать майнкрафт
7	игры	18	инстаграм
8	Гдз	19	калькулятор
9	алиэкспресс		
10	вконтакте		
11	мультки		

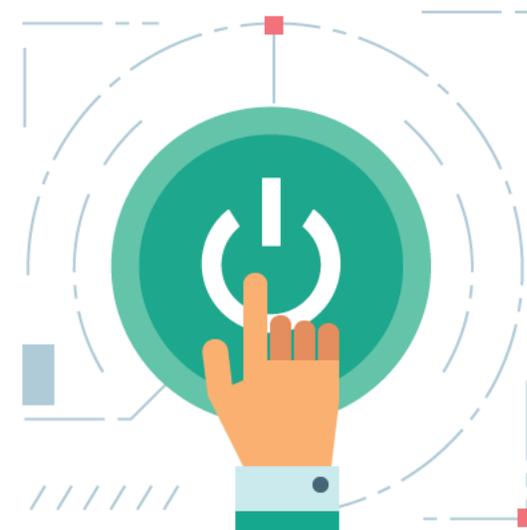


\*Статистика облачного сервиса Kaspersky Security Network. Посещения различных интернет-ресурсов при включенном «Родительском контроле» на ПК в России. Усредненный показатель за последние 6 месяцев.

# ВЕБ СЕРФИНГ: ЗАДАНИЕ ИЗ ПОСОБИЯ

**Задание:** Разделитесь на группы по 3 – 4 человека. Распределите по два сервиса из предложенных ниже на каждую группу. Найдите в интернете всю возможную информацию о фишинговых атаках, нацеленных на пользователей этих организаций: скриншоты настоящих сайтов, что из себя представляет компания, для чего фишерам нужно проводить на нее атаки, скриншоты сайтов-подделок, статистика (например, какое место эта компания занимает среди атакуемых фишерами), истории пользователей и как организация старается защищать своих пользователей от мошенников). На основе полученного материала расскажите о выбранных вашей группой двух организациях, на чьих пользователей часто проводятся фишинговые атаки, в удобном для вас формате – презентация, рисунки на флипчарте или на обычных листах А4:

Facebook  
Vkontakte  
Booking  
Aliexpress  
Google  
.....



# Социальные сети

# СОЦИАЛЬНЫЕ СЕТИ



У **40%** детей в младшей школе **уже** есть страница в соцсетях. Среди старшеклассников этот показатель возрастает до **97%**.



**70%** школьников получают приглашения дружить от незнакомых людей. При этом **18%** школьников получают приглашения от незнакомых **взрослых**.



Количество детей, получающих приглашения от незнакомых взрослых, **резко возрастает** в возрасте **10-12 лет**.



**Каждый десятый** школьник имел опыт встречи с людьми, с которыми он/она познакомился в соцсетях.



**21%** школьников имеют друзей/одноклассников, которые смотрят или постят жестокие видео или записи. При этом чаще всего о таких в своем окружении говорят дети **13-15 лет**.



# НАИВНОСТЬ ДЕТЕЙ И ОВЕРШЕРИНГ



Написать сообщение



Добавить в друзья



Мargarita Евгеньевна Вилакова

заходила сегд



День рождения: 14 октября 2000 г.  
Город: Калининград  
Семейное положение: в активном поиске  
Место работы: Медиахолдинг| Гимназия №40  
Скрыть подробную информацию

## Основная информация

Родной город: мурманск  
Языки: Русский, Български, English  
Братья, сестры: Вера Латышева, Алевтина Святая

## Контактная информация

Моб. телефон: +79210410046  
Skype: Ritka3951  
Instagram: margaritavil15  
Дом: Burgas в 2011 г.

## Карьера

Место работы: Медиахолдинг| Гимназия №40  
Калининград

## Образование

Школа: Гимназия №40  
Калининград, 2015–2017 (н)  
Физ-мат



Написать сообщение



Добавить в друзья



Виола Новикова

заходила вчера в 2

Сырок Виола★ INST: @viilaa\_sa

День рождения: 15 июля 2004 г.  
Город: Калининград  
Место учёбы: Школа №38

72  
друга

322  
подписчика

72  
фотографии

2  
видеозаписи

## Фотографии Виолы 72

Алина Матонина

День рождения: 20 октября  
Город: Калининград

295  
друзей

330  
подписчиков

21  
фотография

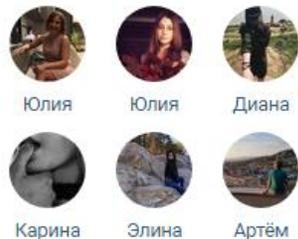
11  
видеозаписей

## Фотографии Алины 21



Друзья 396

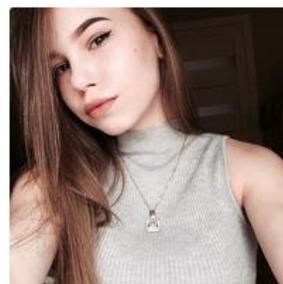
новости



Подарки 352



Отправить подарок



Отправить подарок

Добавить в друзья



Друзья 295

новости



# ПРИВЕТ ОТ НЕЗНАКОМЦА



XXX

> Привет, Саш, скинь плиз номер телефона, есть разговор

XXX

> дарова  
> классный коммент в [паблик]  
> я прям проорал)))0  
> давай знакомиться?

XXX

> Привет!  
> классные фотки, ты дико красивая! Добавишь в друзья?

XXX

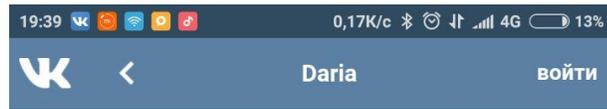
> прив  
> это Настя из 8Б, давай погуляем  
> давай я за тобой зайду, напомнишь адрес?  
> кстати, родки дома?

XXX

> слушай, мы с тобой уже месяц общаемся  
> может, го в мақдаке посидим?

**НЕ УВЕРЕН – СПРОСИ У РОДИТЕЛЕЙ!**

# БЕЗОПАСНОЕ ОБЩЕНИЕ В СЕТИ, ОВЕРШЕРИНГ



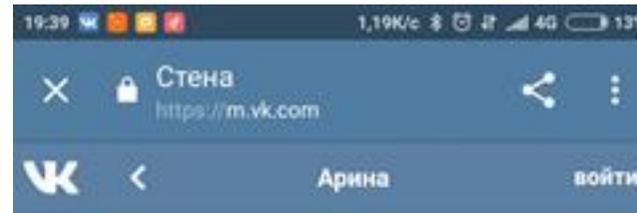
 **Daria Fukushima**  
21 фев 2016 в 13:16

Утро бывает добрым... ☀️🔥❄️  
P.s. Когда мама улетает в Германию и оставляет дочь одну @ Москва, ЦАО



 улица Серпуховский Вал, Москва

 Понравилось 15 людям

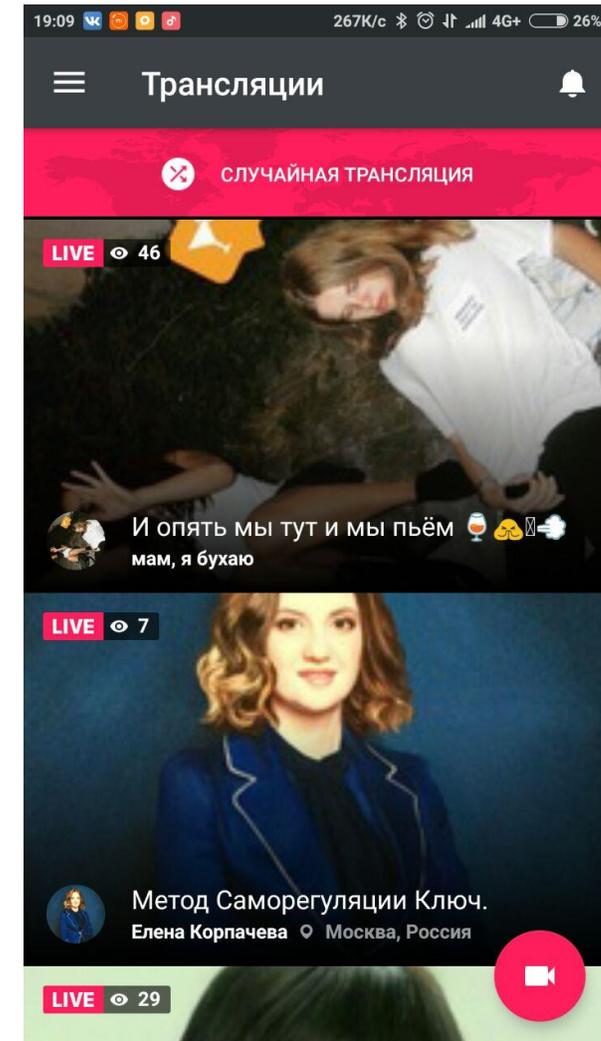


 **Арина Тупкало**  
30 апр 2013 в 21:41

В 6:00 улетаю в Турцию



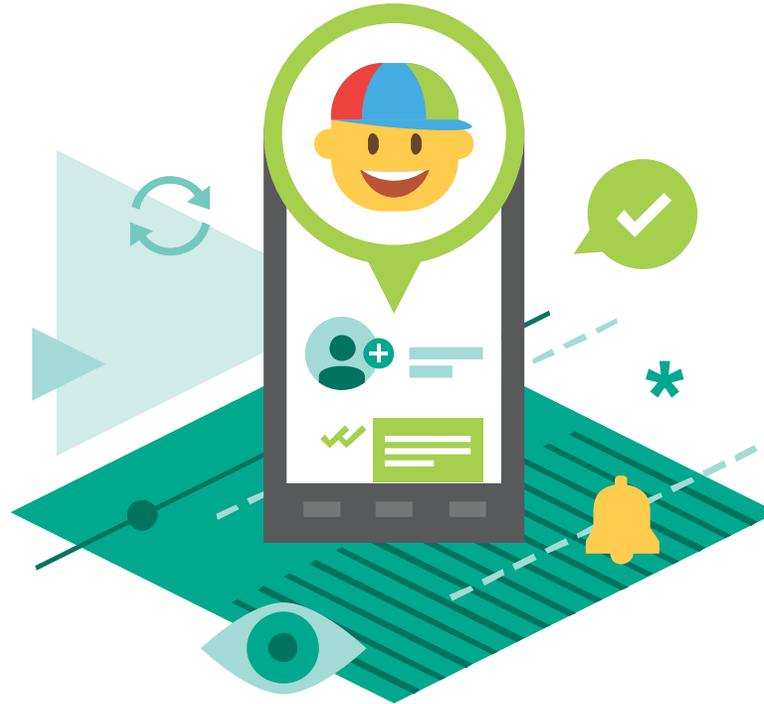
улица Ленина  
Молоково



# ПРОСТЫЕ ПРАВИЛА

## Правило трех секунд

- Если ты написал пост, не жми сразу на кнопку «Опубликовать»! Досчитай до трех и задай себе три вопроса:
- 1) Хочу ли я, чтобы это прочитали все-все-все: родители, учителя, друзья, одноклассники, я через десять лет, мои будущие однокурсники в университете?
  - 2) Не будет ли кому-то обидно или неприятно это читать?
  - 3) Готов ли я написать это на футболке, в которой буду везде ходить?



## Правило мамы

- Перед тем, как опубликовать пост, фотку или еще что-нибудь, подумай: а что бы сказали мама, папа или классный руководитель, если бы увидели?
- Если чувствуешь, что не хотел бы, чтобы они увидели, значит, с твоим постом что-то не так...

# ВПИСКИ



Вписки Калининграда | Вписки Калининград

Вступить

Товары 2



Реклама  
50 руб.



Разбан  
40 руб.



Добавить запись...



ВПИСКА В КАЛИНИНГРАДЕ | VVK

2 авг в 12:10

отдохнули вчера с подружками урааа лето)))  
анонимно



🔔 Включить уведомления

★ Добавить в избранное

Участники 888



Александр



Елизавета



Александр



Юрий



👁 186



Уголовный Розыск  
Доиграетесь мне!

4 авг в 3:11 Ответить

❤ 1

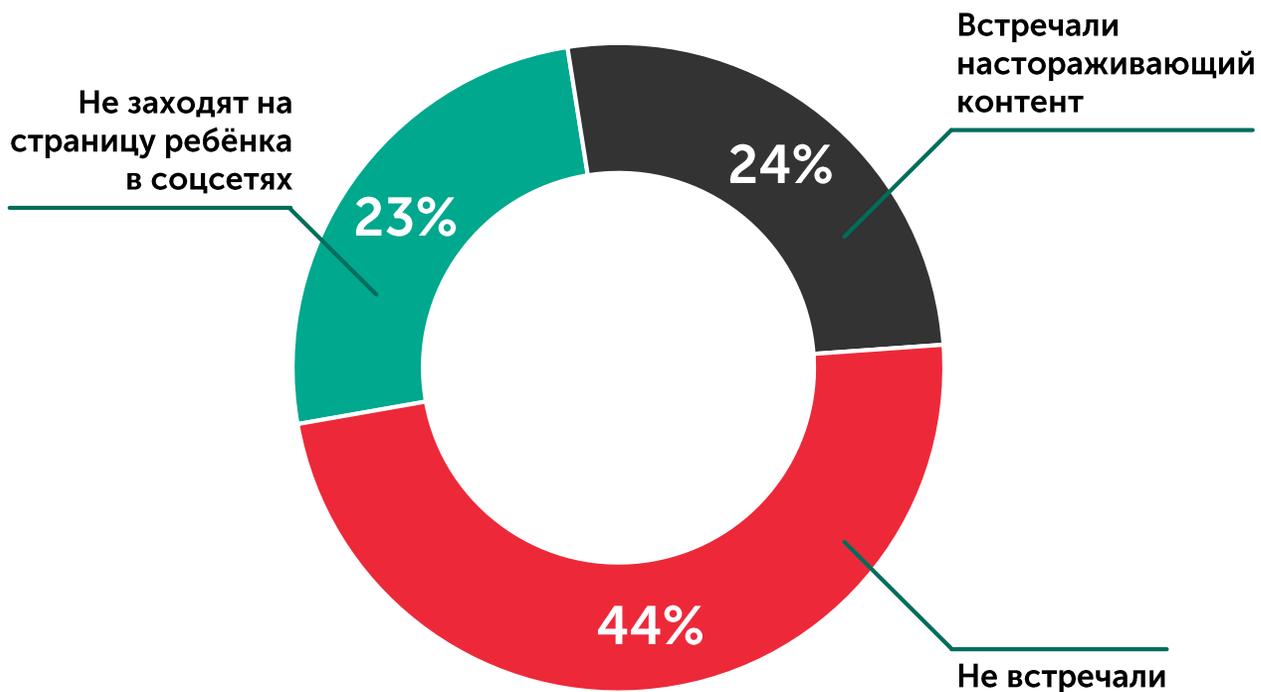
# СОЦИАЛЬНЫЕ СЕТИ: РЕАКЦИЯ РОДИТЕЛЕЙ



**Практически четверть** родителей школьников встречает что-то настораживающее на страницах своих детей в соцсетях. Чаще всего это случается в семьях с детьми **13-15 лет**.

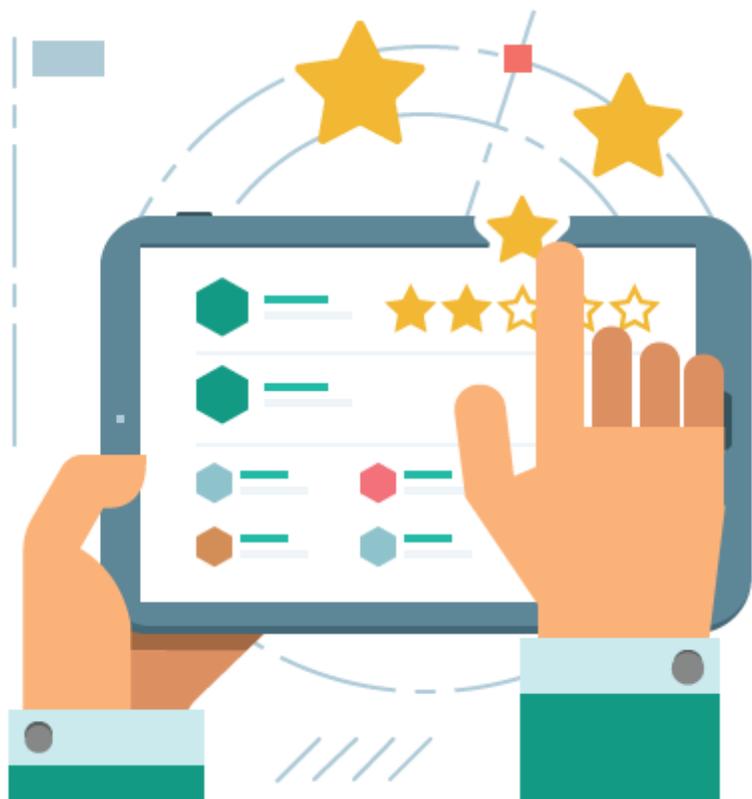


В основном родителям не нравятся или тревожат **люди**, с которыми ребенок общается. На втором и третьем месте **пабрики**, на которые ребенок подписан, и **посты**, которые ребенок публикует / «шарит».



# ЧТО МЫ РАССКАЗЫВАЕМ, КОГДА РАССКАЗЫВАЕМ?

Не обо всем нужно рассказывать в интернете!



Саша

Вторник, 10:15

сходили только что на Пилу, топовый фильм!

Саша

Вторник, 17:36

добавляемся в стиме, ник dota\_rush\_mid

Саша

Пятница, 16:11

пацаны выиграли у 285 школы в футбол, молодцы, школа 1543 топ!

Саша

Суббота, 21:25

завтра наконец-то мне 14, кст видел, как мама заказывает айфон десятку, угадайте, кому)))

📍 Москва, ул. Ясная, д. 5

Саша

Воскресенье, 16:11

в понедельник улетаем в Сочи на неделю, всем пока, ждите фоток с айфона. Инета не будет, пишите на

+79998887766

# СОЦИАЛЬНЫЕ СЕТИ: ЗАДАНИЕ ИЗ ПОСОБИЯ

**Задание:** Разделитесь на группы по 3 – 4 человека. Распределите по группам следующие вопросы по одному на каждую группу. У групп есть 5 минут на обсуждение полученного вопроса и 2 минуты на презентацию своей позиции в классе. Можете записать ключевые мысли на лист А4.

- Чем опасно общение с незнакомыми людьми в социальных сетях?
- Можно ли публиковать все, что угодно, если доступ к твоему аккаунту есть только у друзей?
- При каких условиях можно общаться с незнакомыми людьми в интернете?
- Допустимы ли встречи с незнакомыми людьми, с которыми ты общаешься только в интернете?
- Представьте свою позицию классу и обсудите ее все вместе.



# Кибербуллинг

# КИБЕРБУЛЛИНГ ИЛИ БУЛЛИНГ

<http://detionline.com/helpline/about>

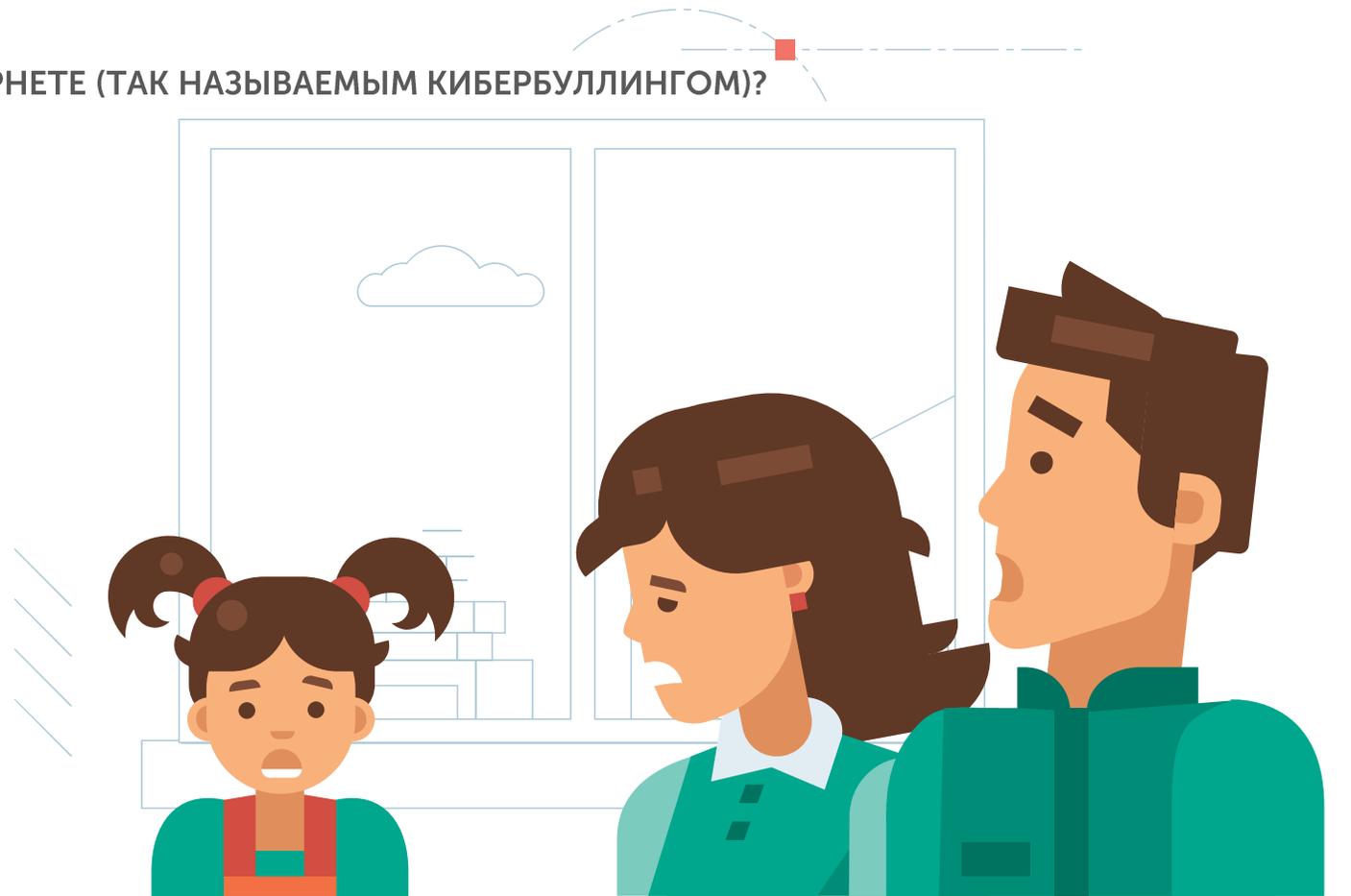


# КИБЕРБУЛЛИНГ



**Каждый десятый** родитель отмечает, что тема кибербуллинга в той или иной степени ему знакома. Чаще всего рапортуется о случаях в школе, реже – среди друзей ребенка. Данный показатель не зависит ни от возраста, ни от пола ребенка.

СТАЛКИВАЛСЯ ЛИ ВАШ РЕБЕНОК С ТРАВЛЕЙ В ИНТЕРНЕТЕ (ТАК НАЗЫВАЕМЫМ КИБЕРБУЛЛИНГОМ)?



# КИБЕРБУЛЛИНГ



Если же задать вопрос про травлю детям, то доля тех, кто сталкивался с кибербуллингом либо слышал о нем, возрастает более, чем в два раза (со слов родителей – **12% vs 29%** – со слов детей).

## ВОПРОС О КИБЕРБУЛЛИНГЕ, ЗАДАННЫЙ ДЕТЯМ



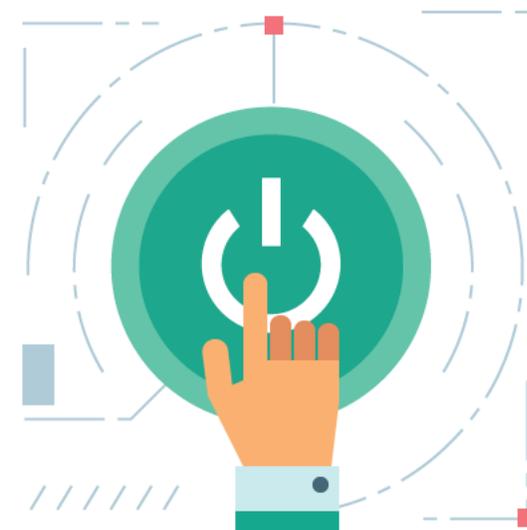
# КИБЕРБУЛЛИНИГ: ЗАДАНИЕ ИЗ ПОСОБИЯ

**Задание:** Лучшее средство от кибербуллинга – поддержка со стороны друзей и знакомых, осознание того, что ты гораздо лучше, чем пишут твои обидчики. В процессе этого проекта мы создадим группу поддержки для каждого из вас. Потребуется небольшая подготовка, если вы не делали этого раньше: нужно установить на смартфон каждого из вас мессенджер (whatsapp, viber, threma или любой другой, но для всех одинаковый) и узнать номера телефонов всех в вашем классе.

Пусть каждый из вас создаст в мессенджере группу. Назовет ее своей фамилией в дательном падеже («Иванову», или «Петрову»). Если у тебя в классе есть родственники или однофамильцы, добавь первую букву своего имени или имя целиком. В эту группу нужно добавить всех, кто выполняет этот проект.

В результате у каждого из вас в мессенджере будет столько групп, сколько человек посещает наш курс. В каждой из этих групп участниками будут все, посещающие этот курс.

Теперь задача каждого в классе написать в каждый чат, в который его добавили (то есть каждому однокласснику), что-то хорошее, доброе и позитивное, чтобы в случае травли каждый из вас мог вспомнить об этой группе, открыть ее и прочитать слова поддержки.



Что можно сделать?

# Учебный материал, пособия рассчитан на обучающихся 7-9 классов и обеспечивает организацию внеурочной деятельности в основной школе

# Содержание пособия имеет модульную структуру Каждый модуль разделен на разделы и рассчитан на один класс

Чем плоха травля? Тем, что ее жертва получает чаще всего очень серьезную психологическую травму и даже может попытаться навредить себе. Обидчики чаще всего не хотят таких серьезных последствий, а лишь развлекаются, не задумываясь о чувствах жертвы.



Формат травли может быть самым разным. Некоторым детям пишут личные сообщения по всем каналам и публикуют что-то в лентах, других травят в общих группах класса, иногда даже создают отдельные группы, которые посвящают именно тому, чтобы ненавидеть там своего одноклассника.

### Задание 1.

Разделитесь на группы по 3—4 человека. Найдите в Интернете 2—3 истории о кибербуллинге (в новостях, в лентах соцсетей, в блогах и т. д.). Постарайтесь найти хотя бы одну историю со счастливым концом. Представьте найденные вами истории одноклассникам.

На всех популярных сервисах, пароль от которых нуждается в защите, есть возможность настроить безопасность. Что нужно знать о таких настройках?

Обычно перейти к настройкам можно, нажав на значок шестеренки или надпись «Настройки», которая может быть как сама по себе, так и появляться после нажатия на три полоски.



### Задание 1.

Работая в группах по 3—4 человека, выберите 10 популярных сервисов, которыми вы активно пользуетесь, зайдите на их сайты данных сервисов или в их мобильные приложения и найдите настройки безопасности (не путайте с приватностью и конфиденциальностью). На листе А4 запишите, как и в каком сервисе вы попали в эти настройки: как выглядела иконка для перехода, какие шаги нужно сделать, чтобы попасть непосредственно к настройкам безопасности.

## 2.2 ФИШИНГОВЫЕ ПИСЬМА

На прошлом уроке мы обсудили самые простые приемы фишеров — письма, в которых они просят прислать пароль в ответ на их письмо или заполнить форму прямо внутри письма.



Доменная зона, или домен первого уровня, часто указывает на страну, в которой расположен сайт, но не всегда. Есть глобальные зоны, к примеру .net, .com, .org, к тому же обычно не составляет труда зарегистрировать адрес в доменной зоне государства, гражданином которого ты не являешься.

Но есть и более сложные приемы, которые бывает сложнее раскрыть пользователю. Обычно формы в них очень похожи на формы в честных письмах или пользователю предлагается перейти на сайт, чтобы ввести там логин и пароль. Все данные, введенные на таких сайтах или в таких формах, будут отправлены злоумышленникам. На предыдущем уроке мы искали отличия между честными и мошенническими письмами, и порой это было довольно сложно сделать, поскольку злоумышленники стараются сделать свои сообщения очень похожими на те, что присылают большие честные сервисы.

Чтобы как следует разобраться в том, как фишеры создают такие сообщения, на которые с удовольствием отвечают пользователи, посмотрим, что именно и как им удается подделывать.

<b>РАЗДЕЛ 1. Вредоносный код</b>	<b>6</b>
1.1. Что такое вредоносный код	6
1.2. Возможности вредоносных программ. Интернет вещей	10
1.3. Возможности вредоносных программ. Умный город	11
1.4. Возможности вредоносных программ. Актуальный ландшафт	13
1.5. Возможности вредоносных программ. Актуальный ландшафт. Продолжение	14
1.6. Возможности вредоносных программ. Дополнительные функции	16
1.7. Как распространяется ВПО. Спам	18
1.8. Как распространяется ВПО. Спам. Исполняемое содержимое	20
1.9. Как распространяется ВПО. Скачай сам	21
1.10. Как распространяется ВПО. Скачай сам. Продолжение	22
1.11. Как распространяется ВПО. Другие пути	24
<b>РАЗДЕЛ 2. Фишинг</b>	<b>26</b>
2.1. Что такое фишинг?	26
2.2. Фишинговые письма	29
2.3. Фишинговые сайты	31
2.4. Фишинг в соцсетях и мессенджерах	33
2.5. Нигерийские письма	35
2.6. Что делать? Защищай свой пароль	37
2.7. Как придумать сложный пароль	39
2.8. Настройки безопасности в популярных сервисах	41
<b>РАЗДЕЛ 3. Основы защиты ПК</b>	<b>44</b>
3.1. Антивирусные программы	44
3.2. Обновления ОС, лицензионного ПО и антивируса	46
<b>РАЗДЕЛ 4. Общение в социальных сетях</b>	<b>45</b>
4.1. Личное общение в соцсетях и мессенджерах	45
4.2. Соцсети. Персональные данные	50
4.3. Чем еще нельзя делиться в соцсети	53
4.4. С кем и как мы общаемся в Интернете	54
4.5. Настройки конфиденциальности в соцсети	55
4.6. Кибербуллинг	57

# Предлагаемое пособие реализует требования ФГОС

## по предмету ОБЖ

Защита от мошенников (в сети), информационная безопасность при использовании компьютера, мобильного телефона, при просмотре телевизионных программ и пользования Интернетом, защита личной, семейной (персональной) информации

<b>РАЗДЕЛ 2. Фишинг</b> .....	26
2.1 Что такое фишинг? .....	26
2.2 Фишинговые письма .....	28
2.3 Фишинговые сайты .....	31
2.4 Фишинг в соцсетях и мессенджерах .....	33
2.5 Нигерийские письма .....	35
2.6 Что делать? Защищай свой пароль .....	37
2.7 Как придумать сложный пароль .....	39
2.8 Настройки безопасности в популярных сервисах .....	41
<b>РАЗДЕЛ 3. Основы защиты ПК</b> .....	44
3.1 Антивирусные программы .....	44
3.2 Обновления ОС, лицензионного ПО и антивируса .....	46

## по предмету Информатика

вопросы повышения безопасности работы в Интернете, взаимодействия на основе компьютерных сетей:  
электронная почта, чат, форум, др.  
базовые представления о правовых и этических аспектах работы в Интернете, личной информации и способах ее защиты

<b>РАЗДЕЛ 4. Общение в социальных сетях</b> .....	48
4.1 Личное общение в соцсетях и мессенджерах .....	48
4.2 Соцсети. Персональные данные .....	50
4.3 Чем еще нельзя делиться в соцсети .....	53
4.4 С кем и как мы общаемся в Интернете .....	54
4.5 Настройки конфиденциальности в соцсети .....	55
4.6 Кибербуллинг .....	57

# УЧЕБНЫЕ ЗАНЯТИЯ

## ПРЕДЛОЖЕНЫ В ФОРМЕ ИНДИВИДУАЛЬНОЙ И ГРУППОВОЙ РАБОТЫ, ПРАКТИЧЕСКИХ РАБОТ, УЧЕБНЫХ ПРОЕКТОВ, МАСТЕР-КЛАССОВ

### Задание 2.

Работая в группах по 3—4 человека, постарайтесь найти в Интернете 3—4 группы в известных соцсетях, созданные для кибербуллинга, или группы, созданные для того, чтобы найти людей, которые помогут в травле (есть и такие!). Представьте эти группы и обсудите в классе то, что вы увидели. Соответствует ли такое поведение в Сети нормам поведения в обществе?

### Задание

Разделитесь на группы по 4—5 человек и на листе А4 за 10 минут создайте максимально полный список информации, которой опасно делиться в социальной сети. К каждому приведенному вами пункту найдите 1—2 примера на страницах пользователей «ВКонтакте» и сделайте скриншоты. Создайте общий список опасностей, предложенных вашим классом. Для этого все группы по очереди должны представить по одному пункту из своего списка, пока у всех групп не закончатся варианты.



### Задание 3.

Придумайте пароль, который состоит из 7—8 букв, одного символа (например, ? \* # % \$ и т. д.) и 2—3 цифр. На листе А4 зашифруйте свой пароль в форме ребуса. Представьте ребус классу, пусть одноклассники попробуют его отгадать.



### Проект

Разделитесь на группы по 3—4 человека. Составьте список возможных путей попадания вредоносной программы на компьютер пользователя. Напишите рекомендации для каждого из этих путей: что должен делать пользователь, чтобы не подцепить таким образом вредоносную программу. Представьте свой список в классе. Составьте общие рекомендации вашего класса для того, чтобы избежать заражения компьютера вредоносным кодом.

# ПРИМЕРЫ ПРОБЛЕМ

## ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОСОБИИ

Вредоносная активность современных программ нацелена чаще всего на кражу финансовых данных пользователя, чтобы получить доступ к его банковским счетам, или на кражу логинов и паролей от популярных сервисов. Кроме того, спросом пользуются персональные данные пользователей, например фотографии паспортов, которые пользователи часто хранят на своих компьютерах. Такие данные преступники часто продают на черном рынке.



В конечном счете цель фишинга — деньги. Фишинг используют, чтобы добраться либо до ваших денег, либо до вашей личной информации, которую можно потом продать или воспользоваться ею, чтобы украсть у вас деньги.

Есть такой интересный вид интернет-мошенничества — нигерийские письма. Он не похож на классический фишинг, поскольку злоумышленникам не требуются никакие логины или пароли, эта схема подразумевает прямой отбор денег у жертвы.

Второе, что возможно сделать в настройках безопасности, — включить двухфакторную аутентификацию на вашем аккаунте.

Основных отличий онлайн-травли от травли в реальности два:

1. Ее долго могут не замечать взрослые, из-за чего в случае особенно острых конфликтов могут вмешаться слишком поздно.
2. Она не заканчивается, когда жертва уходит домой из школы, — обидчики всегда «с тобой»: в смартфоне, планшете и других устройствах.



Пароль — это то, что защищает информацию, которую вы размещаете в ваших аккаунтах в Интернете. Пароль будет выполнять свою функцию, только если посторонние не будут иметь к нему доступа.



<https://kids.kaspersky.ru/category/entertainment>

<https://shop.prosv.ru/>