

# **Методические рекомендации для педагогов по теме «Информационная безопасность в образовательном процессе»**

**Авторы разработчики:**  
**Сахарова Е.В., учитель начальных классов;**  
**Чуева С.А., учитель технологии**

В настоящее время практически все люди в той или иной степени сталкиваются с разнообразными видами мошенничества. В зоне риска оказываются практически все: от детей начальной школы до людей пенсионного возраста.

В нашей статье мы рассмотрим некоторые моменты, связанные с различными мошенническими действиями. Основное внимание мы уделим мошенническим действиям и противодействию им в рамках образовательного процесса.

***Остановимся на следующих моментах:***

- 1. Участники образовательного процесса (краткая характеристика каждой из групп).***
- 2. Типичные ситуации мошенничества для каждой из групп, факторы риска.***
- 3. Учителя и сотрудники образовательных учреждений как особая группа риска.***
- 4. Противодействие мошенническим действиям.***
- 5. Статистика наиболее типичных ситуаций мошеннических действий по нашему региону.***

## ***1. Участники образовательного процесса (краткая характеристика каждой из групп).***

Основными участниками образовательного процесса являются три категории: учителя, родители и дети.

Остановимся на кратких характеристиках каждой из групп.

Учителя: очень разновозрастная категория, высокоориентированная на профессиональную деятельность, в связи с чем некоторые социальные события в обществе остаются вне зоны внимания. Возраст сотрудников современных образовательных учреждений: от 20 лет до 70+.

Родители: очень разноплановая категория – от глубоко заинтересованных в участии в учебном процессе до совершенно отвлеченных от проблем обучения своих детей. Основным интерес у большинства представителей данной группы – профессиональная деятельность. Возраст родительской аудитории в среднем от 27-30 лет до 50+.

Дети: разновозрастная категория, которая охватывает период от младшего школьного возраста до юности. Чем старше представители этой категории, тем шире спектр их интересов. Однако, практически с самого начала школьного возраста дети демонстрируют явную зависимость от различных гаджетов и социальных сетей. Возраст представителей данной группы: от 7 до 18 лет.

## ***2. Типичные ситуации мошенничества для каждой из групп, факторы риска.***

В данном разделе мы предприняли попытку систематизировать в таблице наиболее типичные ситуации мошеннических действий. Данные взяты нами из статей на эту тему в интернете, а также из официальных новостных каналов нашей области («Жесть Рыбинска», «Это случилось в Рыбинске», «Жесть Ярославской области» и др.)

| Типы<br>мошеннических<br>действий                   | Категории участников образовательного процесса                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |          |                                                                                                                                                                                                                                                             |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     | Учителя                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Родители | Дети                                                                                                                                                                                                                                                        |
| <b>Общие ситуации</b>                               | <b>Мошенники:</b> <ul style="list-style-type: none"> <li>- фальшивые призы;</li> <li>- вредоносные программы;</li> <li>- спасение семьи от уголовного или административного преследования;</li> <li>- просьба виртуального друга;</li> <li>- ошибочный платеж (просьба вернуть случайные деньги, при этом мошенник получает доступ к банковскому приложению);</li> <li>- попытки уточнить данные документов (паспорт, данные банковских карт и т.п.) от лица различных организаций.</li> </ul>                                                                                                                       |          |                                                                                                                                                                                                                                                             |
|                                                     | <b>Вербовщики:</b> <ul style="list-style-type: none"> <li>- запугивание разного рода (человек заподозрен в противоправной деятельности и находится в разработке спецслужб);</li> <li>- вредоносные программы (пошли по ссылке на профессиональную тему, попали на запрещенный сайт);</li> <li>- легкая работа (например, писать левые отзывы на товар);</li> <li>- покупки за слишком маленькую цену (как следствие бесконечные предложения и формирование зависимости от якобы «выгодных покупок»);</li> <li>- виртуальные задания (выполняется некая работа, но при переводе на карту деньги исчезают).</li> </ul> |          |                                                                                                                                                                                                                                                             |
| <b>Ситуации, ориентированные на каждую из групп</b> | <ul style="list-style-type: none"> <li>- звонки от руководства;</li> <li>- случайные люди в профессиональных чатах;</li> <li>- «левые» ссылки на профессиональную тему;</li> <li>- фишинговые ссылки;</li> <li>- спасение средств (перевод на безопасные счета);</li> <li>- быстрая большая прибыль (финансовые пирамиды);</li> <li>- промежуточные счета (участие дропперов – подставных лиц);</li> <li>- случайные кредиты.</li> </ul>                                                                                                                                                                             |          | <ul style="list-style-type: none"> <li>- легкий доход в играх или покупка дополнительных опций в играх;</li> <li>- быстрый заработок на нужную вещь;</li> <li>- обращения из школы (секретарь, медсестра);</li> <li>- аренда аккаунтов или карт.</li> </ul> |

### 3. Учителя и сотрудники образовательных учреждений как особая группа риска.

В данной части нашей статьи мы попытались описать и систематизировать основные особенности учителей разных возрастных групп для понимания наиболее очевидных факторов риска для каждого возраста.

#### **Группа 1: Молодые специалисты (возраст до 30 лет)**

Представители данной группы - люди, которых отличает преимущественно оптимистический настрой на жизнь, коммуникабельность, творческий подход, умение использовать новые методы и современные технические средства обучения. Кроме всего прочего, такие люди обладают достаточно высокой адаптивностью и находятся «на одной волне» со своими учениками.

Вместе с этим некоторые представители этой группы демонстрируют отсутствие терпения, категоричность в своих взглядах и нежелание принимать прошлый опыт. Все это приводит к затруднениям в общении с учениками, родителями и коллегами старших возрастных групп.

Молодые специалисты ведут активный образ жизни: контактируют в социальных сетях с разными людьми, имеют свои странички или даже авторские группы, связанные с профессией или хобби, активно используют все бонусные возможности банковских и скидочных карт. Они заинтересованы в совершении экономических покупок и дополнительном заработке с минимальными затратами сил.

Основными факторами риска для данной возрастной группы являются мошеннические действия в интернет пространстве.

Мошенники предлагают приобрести что-то за низкую цену в обмен на указание личных данных, обещают спасти и обезопасить счета или избавить от кредита, который берут на имя человека посторонние, пытаются заманить к какую-то деятельность, где можно легко и быстро заработать, угрожают разработками в органах на предмет участия в чем-то запрещенном. Активно используется «обращение друга» (выручи деньгами, закинь деньги на телефон), просьбы проголосовать (переход по вредоносной ссылке) и т.п.

Следует отметить, что молодые специалисты в силу своей активной жизненной позиции в курсе многих новостей из интернет каналов и довольно редко в сравнении с остальными категориями впечатляются обращениями мошенников.

### ***Группа 2: Специалисты среднего возраста (возраст от 30 лет до 50 лет)***

Представители данной группы отличаются очень разным настроением на жизнь: от оптимистических взглядов до разочарования в своих действиях и происходящим вокруг. Могут появиться «первые звоночки» профессиональных деформаций. Тем не менее, эти люди демонстрируют высокий профессионализм, хорошее владение разнообразными методиками преподавания и довольно близкий контакт с детьми. Основными задачами развития являются организация жизни в своей семье, утверждение себя в роли родителя, построение карьеры, выработка собственного стиля жизни.

У некоторых представителей этой группы возраст 35 лет+ совпадает с началом подросткового возраста своих детей. Связанные с этим проблемы неизбежно отражаются на профессиональной деятельности и взаимодействии с окружающими.

После 30 -35 лет происходит переоценка значимости людей. Начинают проявляться первые противоречия между самовосприятием человека и восприятием его окружающими.

Учителя среднего возраста в отношении рисков мошеннических действий во многом совпадают с представителями предыдущей группы. Однако, значительную роль занимают действия мошенников, связанные с потенциальной угрозой детям или другим членам семьи. (Ребенок, муж, брат, сестра и т.п. что-то сделали, можно дело «замять» за некоторую плату).

Далеко не все учителя этой группы в полной мере осведомлены о возможностях банковских и скидочных карт, поэтому мошенники могут ссылаться на неизвестную опцию.

### ***Группа 3: Специалисты старшего возраста (возраст от 50 лет)***

Источник энергии в зрелом возрасте – осознанная концепция жизни, глубина познания своих возможностей и потребностей. Стиль жизни человека определяет его жизненная позиция. Учитель «за 50» демонстрирует ответственность, обязательность, пунктуальность, устойчивые установки относительно своего поведения и поведения окружающих (что можно, что нельзя).

Дети вырастают и покидают родительский дом, а значит, важность приобретает установление связей вне семьи (клубы по интересам, участие в деятельности интернет сообществ). Снижается роль работы. Причины могут быть разными: разочарование в профессии, смена профессиональных приоритетов (репетиторство стало важнее), внутренние личностные проблемы и противоречия. Более значимой становится разница во взглядах между учителем и его воспитанниками.

Наряду с профессиональным опытом некоторые учителя этой группы могут демонстрировать несколько несовременные подходы к учебному процессу, затруднения в использовании современных технических средств. Обуславливать ряд проблем в общении и профессиональной деятельности могут и проблемы со здоровьем.

Основные факторы риска здесь: боязнь попасться в разработки органов (что будет с репутацией), страх потерять накопленное, вера в заботу лечебных заведений (вам

звонят/пришли/пишут из поликлиники), вера в лучшее в людях (помощь случайно обратившимся).

#### **4. Противодействие мошенническим действиям.**

Главными условиями противодействия мошеннических действий является следующее;

- не давать никакой личной информации случайным людям;
- быстро сориентироваться и задать какой-то контрольный вопрос (например, звонок от лица коллеги или начальника – спросить то, что вы оба знаете наверняка);
- не переходить по незнакомым ссылкам;
- максимально быстро прекратить разговор, в котором у вас пытаются выведать какую-то личную информацию;
- «расколоть» мошенника, можно использовать метод провокации: опередив собеседника, сообщить ему, что «есть проблемы с картой, списываются деньги, звонивший намерен помочь»; при этом нужно избегать излишне агрессивных действий; мошенники же, напротив, зачастую срываются, хамят, даже обзывают, выдавая тем самым себя безоговорочно;
- стараться как можно меньше говорить с позвонившим мошенником, даже, если разговор идет на безобидные темы (помните, что ваши ответы могут быть записаны, а далее преобразованы в нужную мошеннику аудиозапись);
- следует помнить, что никакие сотрудники банка, спецслужб, представители сетевых магазинов (типа Магнит, Пятерочка и т.п.) не позвонят вам для уточнения личных данных;
- если вам позвонили от лица знакомого, попавшего в беду, прервите разговор и обязательно перезвоните человеку или тому, кто обязательно должен знать все о том, из-за кого звонили;
- помните, никакие представители спецслужб никогда не повезут вас в банк для спасения денег со счета, а представителям поликлиник совершенно некогда ходить по домам и предлагать массаж на дому или очень полезные пищевые добавки по низкой цене.

#### **5. Статистика наиболее типичных ситуаций мошеннических действий по нашему региону.**

По сведениям новостных каналов лидирующее положение в нашей области занимают мошеннические схемы по спасению сбережений. Алгоритм действий может быть разным: от обращений работников банка или спецслужб с настоятельными рекомендациями перевести деньги на безопасный счет или обналить их и передать конкретному человеку до обвинений в пособничестве лицам, которые совершают противоправные действия. В ряде случаев на связь выходят от лица руководства, создав страницы – дубли.

Итог один – человек теряет средства, и вернуть их не представляется возможным.

Весной 2025 года в городе Рыбинске произошла резонансная история. Сотрудница одного из медучреждений по настоянию «руководителя» (было получено сообщение с «левой» страницы) начала общаться с мошенниками и перевела им крупную сумму денег. С начала 2025 года пенсионеры и даже сравнительно молодые жители Ярославской области регулярно становились жертвами преступников. По сведениям новостного канала «Жесть Ярославской области» одна из самых крупных краж у пенсионера – около 3 млн рублей, переданных злоумышленникам.

К сожалению, наш лицей мошенники тоже не обошли своим вниманием. Регулярно на связь выходят двойники директора и его заместителей с просьбами уделить внимание сотрудникам спецслужб, которые должны выйти на связь. Так одной учительнице, со счета которой якобы пытались перевести деньги для помощи экстремистским организациям, мошенники для убедительности предъявили даже скан постановления с синей печатью о том, что она находится в разработке спецорганов. Женщина не поверила мошенникам и обратилась в полицию. Другая сотрудница, задав контрольный вопрос о своей учебной нагрузке двойнику завуча, по нелепому ответу легко вычислила мошенника и прекратила общение с ним.

Активны также представители различных организаций: сотрудники поликлиник, общественных организаций, фондов и т.п. Эти мошенники либо предлагают товары или услуги

по завышенным ценам, либо пытаются проникнуть в дом престарелых людей и украсть денежные средства.

В начале октября этого года в городе Рыбинске задержаны двое мошенников, которые представляясь сотрудниками поликлиники, проникали в дома пожилых людей (порой оказывая давление и применяя силу) и настойчиво предлагали услуги в виде массажа на дому за символическую плату. Далее они отвлекали хозяина квартиры, когда тот отправлялся за деньгами, и воровали денежные средства.

На территории региона зафиксированы также и факты мошенничества с участием детей. В одних случаях дети «спасая» деньги семьи переводили средства на счета мошенников по их инструкции, в других покупали дополнительные возможности и опции в компьютерных играх. Также ребятам разного возраста даже в каникулярное время в личные сообщения регулярно писали секретари и медработники школ.

В городе Ярославле был зафиксирован случай, когда ребенок, приобретая дополнительные возможности в игре, перевел мошенниками более 80 тыс. рублей.

Учащимся лицея также в летнее время регулярно приходили сообщения от медработника. И только своевременная профилактическая работа помогла избежать плачевных последствий. На удочку мошенников никто не попался.

Какие бы люди не выходили на связь, всегда следует помнить, что любую информацию необходимо проверить прежде, чем предпринимать конкретные действия.

И, конечно же, нужно следить за новостями города и региона, чтобы быть в курсе новых мошеннических схем.

Предупрежден – значит вооружен.

## **Информационная безопасность – педагогическим работникам**

Методические рекомендации и информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников.

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность.

Информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;

ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности - не более одного

урока, а при наличии противопоказаний офтальмолога - только 10 минут, не более 3 раз в неделю;

лучше работать за компьютером в первой половине дня;

комната должна быть хорошо освещена;

при работе за компьютером следить за осанкой, мебель должна соответствовать росту;

расстояние от глаз до монитора - 60 см;

периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами в структуру основной образовательной программы включена программа воспитания, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди студентов пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиабезопасности»); знакомить родителей с современными программно-техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.

В качестве возможного варианта предоставления учащимся соответствующих знаний может быть использована учебная программа «Интернет: возможности, компетенции, безопасность», разработанной специалистами факультета психологии МГУ им. М.В. Ломоносова, Федерального института развития образования и Фонда Развития Интернет, рекомендованная Министерством образования и науки РФ

(<http://detionline.com> - главная страница,

<http://detionline.com/internet-project/about> - теория,

[http://detionline.com/assets/files/research/Book\\_Praktikum.pdf](http://detionline.com/assets/files/research/Book_Praktikum.pdf) — практика).

Содержание программы направлено на обучение учащихся полезному и безопасному использованию сети Интернет и социальных сетей, обучению критической оценке онлайн контента и навыкам сетевой коммуникации. Авторами программы разработано методическое пособие для преподавателей и практикумы для проведения уроков, а также запущен интернет-ресурс «Разбираем Интернет» <http://www.razbiraeminternet.ru>

На этом сайте в игровой форме представлены мультимедийные средства обучения для детей и подростков, надо рекомендовать обучающимся посещать этот сайт.

Содержательная часть и объем учебного курса может определяться индивидуально, в зависимости от потребностей конкретной общеобразовательной организации и учащихся. Обучение навыкам

безопасного и эффективного использования интернет-ресурсов возможно в рамках учебного курса «Основы безопасности жизнедеятельности» и в рамках программ факультативов, кружков, элективных курсов, а также индивидуальных учебных планов, реализуемых образовательными организациями. Материалы бесплатны и доступны для скачивания [www.razbiraeminternet.ru/teacher](http://www.razbiraeminternet.ru/teacher).

Академией повышения квалификации и профессиональной переподготовки работников образования (г.Москва) разработан учебно-методический комплект «Здоровье и безопасность детей в мире компьютерных технологий и Интернет». УМК разработан с учетом потребностей образовательных организаций в области безопасной работы в Интернет и ориентирован на руководителей, методистов, педагогов, заинтересованных в повышении своей компетентности в области безопасного применения ИКТ. Методическое приложение к программе можно использовать при организации просветительской работы с родителями и учащимися.

<https://edu.tatar.ru/upload/images/files/children health and care in it.pdf>

Рекомендации по безопасному использованию Интернета для несовершеннолетних и их родителей даны и на сайте Майкрософт <http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>, <http://www.microsoft.com/ru-ru/security/default.aspx>.

Вышеуказанные сетевые ресурсы могут быть использованы для проведения педсоветов в образовательных организациях по вопросам безопасности детей в сети Интернет.

Рекомендуется провести анкетирование обучающихся и родителей по вопросам безопасного использования сети Интернет. Вопросы для анкетирования учащихся и родителей представлены на сайте «Детионлайн» <http://detionline.com/internet-project/competence-research>

Еще в основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайн-игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

познакомить учащихся с ответственным, достойным поведением в Интернете;

рассказать об основных опасностях и правилах безопасного использования сети Интернет;

убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения,

по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;

объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;

убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им;

ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков - трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование контролируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.

Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Обсудите с подростками азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися: рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся.

Для учащихся старших классов при создании материалов по безопасности можно использовать сервисы Интернета для совместной деятельности. Работа команды учащихся в этом случае может проводиться дистанционно. Одним из примеров является схема «Безопасность детей в

Интернете» <http://www.mindmeister.com/ru/12485180/>

Рекомендуем обратить внимание на создание условия для ознакомления с результатами творчества учащихся. Разработанные материалы можно размещать на сайте образовательной организации, в социальных сетях, блогах и сетевых сообществах.

Для эффективной профилактики интернет-зависимости, профилактики националистических проявлений в молодежной среде и устранения риска вовлечения подростков в противоправную деятельность педагогам необходимо проводить разъяснительную и консультационную работу с родителями учащихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в Интернет.

Возможно проведение бесед о работе учащихся в сети Интернет на классных и общеколледжных родительских собраниях или при индивидуальных встречах; информирование через сайт на страничке для родителей. На таких страничках можно разместить рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в Интернете.

Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля».

Родителям могут быть даны следующие рекомендации по формированию у учащихся навыков безопасного поведения в сети Интернет:

Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.

Научите детей не загружать программы, музыку или файлы без вашего разрешения.

Позволяйте заходить на детские сайты только с хорошей репутацией и контролируемым общением.

Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.

Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Единство родительских и педагогических усилий поможет оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

Интернет-ресурсы для педагогических работников:

<http://www.fid.su/projects/deti-v-internete> сайт Фонда Развития Интернет.

<http://www.ligainternet.ru/> Лига безопасного Интернета.

<http://ppt4web.ru/informatika/bezopasnyjj-internet.html> презентации о безопасном Интернете.

<http://www.microsoft.com/ru-ru/security/default.aspx> сайт Центра безопасности Майкрософт.

<http://www.nachalka.com/node/950> Видео «Развлечение и безопасность в Интернете»

<http://i-deti.org/> портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы

<http://сетевичок.рф/> сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности

<http://www.igra-internet.ru/> — онлайн интернет-игра «Изучи Интернет – управляй им»

<http://www.safe-internet.ru/> — сайт Ростелеком «Безопасность детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам

Информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников

<http://www.ligainternet.ru/news/> мероприятия Лиги безопасного интернета.

Лига безопасного интернета — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета

Госдумы РФ по вопросам семьи женщин и детей. Попечительский совет Лиги возглавляет помощник Президента Российской Федерации Игорь Щеголев.

Международный квест по цифровой грамотности «Сетевичок», ориентированный на детей и подростков.

Национальная премия за заслуги компаний и организаций в сфере информационного контента для детей, подростков и молодежи «Премия Сетевичок»

Всероссийское исследование детей и подростков «Образ жизни российских подростков в сети».

Конференция по формированию детского информационного пространства «Сетевичок»

Памятка педагогам по обеспечению информационной безопасности  
обучающихся (воспитанников)

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
4. Проявляйте интерес к «виртуальной» жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.
5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставляйте на посещение проверенных сайтов.
6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.
7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.
8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.
9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.
10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.
11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

## Основные угрозы личной безопасности в Интернете



### Фишинг

Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения

### Мистификация

Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги



### Кража идентификационных сведений

Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

### Нежелательная почта

Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации



## Основные угрозы безопасности компьютера



### Вирусы и программы-черви

Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных

### Программы-трояны

Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений



### Программы-шпионы

Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу

**Защита.** Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.

**Безопасность.** Наше поведение должно защищать от опасностей Интернета.

## Основные угрозы безопасности детей в Интернете

### Киберхулиганы

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей



### Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ



### Неприличный контент

Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить



### Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу

### Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или своей семье



## Основы информационной безопасности детей (памятка для родителей)

1. Приучайте детей вежливости в общении и поведении не только в реальном мире, но и в виртуальном

2. Старайтесь совместно посещать необходимые детям интернет-ресурсы, чтобы избежать ознакомления с вредной информацией, распространяемой посредством рекламы, уведомлений и иных всплывающих окон

3. Установите программные обеспечения, родительский контроль, которые уберегут ваших детей от вредной для них информации

4\*. Обязательно участвуйте при регистрации детей в мессенджерах и социальных сетях и разъясняйте им особенности их использования. Помните, что в социальной сети «ВКонтакте»  регистрация разрешена по достижении возраста 14 лет, «Инстаграм»,  «Тикток»  и «Ютуб»  - 13 лет



5. Предупреждайте детей о том, что далеко не вся информация, распространяемая в сети «Интернет», соответствует действительности. Приучите их советоваться с вами в случае ознакомления с информацией, которая их настораживает или вызывает опасения

6. Настаивайте на том, чтобы дети не делились личной информацией в интернет-ресурсах. В случае, если такая необходимость возникает, дети должны проконсультироваться с вами

8\*. На систематической основе предупреждайте своих детей о том, что нельзя встречаться с друзьями из Интернета, поскольку человек по ту сторону экрана может оказаться вовсе не тем, за кого себя выдает

7. Вместе с обучением детей культуре общения, приучайте их и к уважению чужой собственности - аудио/ фото/ видеоизображений, поскольку незаконное копирование авторского контента равносильно краже

# Памятка

## безопасного поведения и общения в сети Интернет



# Безопасного путешествия в сети!

Сейчас Бараш  
введет pin  
код, и ... (((



Не будь как  
Бараш!!!  
Подумай !

Не знаешь как  
быть?  
Спроси!!!



# Знатоки интернет-безопасности

## ПРАВИЛА ИГРЫ

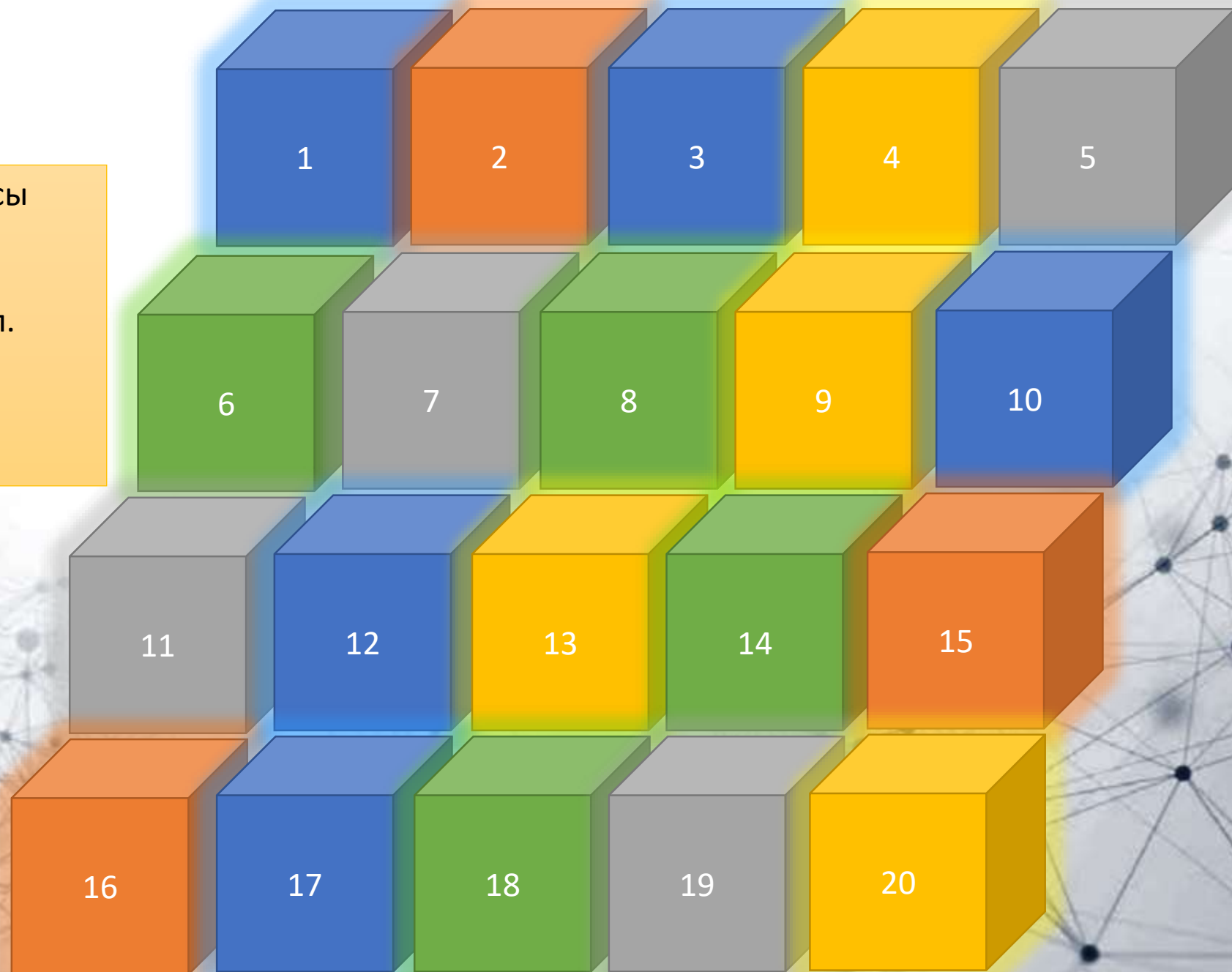
- \*каждый играет за себя или можно объединиться в пары. Для этого в общем чате ученики присваивают себе порядковый номер, затем случайным образом определяются пары и те двое, кто выбирают вопрос;
- \*преимущественное право ответить у того, кто выбирал вопрос, если он(и) не знает ответ, то можно предложить ответить первому, кто выразил свое желание; если ответ верный, то балл засчитывается верно ответившим, если неверный, то ход переходит к следующему по порядку игроку (паре игроков), баллы никому не начисляются, учитель зачитывает правильный ответ со слайда.
- \*время на обдумывание ответа ограничено - не более 30 секунд, так как почти все вопросы предполагают выбор верного варианта из списка.
- \* учет баллов может вести кто-то один из участников, кто, например, не хочет играть, он будет судьей; или учет баллов можно доверить самим игрокам, они могут фиксировать баллы сами в общем чате; также это может делать учитель.

Смелее кубик выбирай и на вопросы отвечай!

Каждый правильный ответ = 1 балл.

В вопросах есть подарки!  
А также дополнительные баллы!

*Завершение  
игры*



Вопрос 1:

Совокупность всей информации, накопленной человечеством в процессе развития науки, культуры, образования и практической деятельности людей – это ...

- ☐ информационные продукты
- ☐ информационные услуги
- ☐ информационные ресурсы

Правильный ответ: информационные ресурсы

← К вопросам

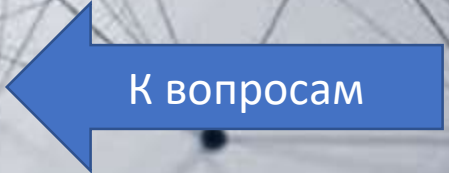
## Вопрос 2:

Под «информационной безопасностью» понимают:

---

- ☐ защиту от несанкционированного доступа
- ☐ защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера
- ☐ защиту информации от компьютерных вирусов

Правильный ответ: защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера



К вопросам

### Вопрос 3:

Какие программы называют эксплойтами?

**Выберите один вариант из списка**

- ☐ вредоносные программы, которые маскируются под полезные
- ☐ те, которые используют уязвимости в программном обеспечении с целью навредить компьютеру
- ☐ программы, которые срабатывают только в определённое время, и, незаметно для пользователя, вредят другим пользователям сети

Правильный ответ: те, которые используют уязвимости а программном обеспечении с целью навредить компьютеру

← К вопросам

Вопрос 4:

Чем трояны отличаются от вирусов?

Выберите один вариант из списка

- ☐ ничем, это одно и то же
- ☐ трояны распространяются самостоятельно, а вирусы распространяет человек
- ☐ трояны распространяют люди, а вирусы распространяются самостоятельно

Правильный ответ: трояны распространяют люди, а вирусы распространяются сами

← К вопросам

## Вопрос 5:

Как известно, злоумышленникам не составляет труда подобрать простой пароль от почты. Именно поэтому, Яндекс.Почта рекомендует создавать сложные пароли. Какой из этих паролей вы не считаете сложным?

Выберите один вариант из списка

- ☐ 23051995 (дата рождения)
- ☐ qwertyasdf567 (пароль, в котором больше восьми символов)
- ☐ Pp1rev04k@ (пароль, в котором есть большие и маленькие буквы, цифры и специальные символы)

Правильный ответ: 23051995 (дата рождения) ++++++ нажми еще раз!

+ подарок 3 балла за правильный ответ!!! Ура!!!

← К вопросам

Вопрос 6:

Что такое двухфакторная аутентификация?

**Выберите один вариант из списка**

- ☐ пароль+одноразовый код
- ☐ связка логин+пароль
- ☐ логин+пароль+контрольный вопрос

Правильный ответ: пароль+одноразовый код

← К вопросам

Вопрос 7:

Что такое фишинг?

Выберите один вариант из списка

- ☐ подбор пароля
- ☐ кража учётных данных с помощью фальшивых сайтов, маскирующихся под настоящие
- ☐ взлом аккаунта с помощью ответа на контрольный вопрос

Правильный ответ: кража учетных данных с помощью фальшивых сайтов, маскирующихся под настоящие

← К вопросам

Вопрос 8:

Что такое брутфорс?

Выберите один вариант из списка

- ☐ подбор пароля
- ☐ кража учётных данных с помощью фальшивых сайтов, маскирующихся под настоящие
- ☐ взлом аккаунта с помощью ответа на контрольный вопрос

Правильный ответ: подбор пароля ++++++ нажми еще раз!

+ подарок 3 балла за правильный ответ!!! Ура!!!

← К вопросам

Вопрос 9:

Что нужно делать, когда вы заходите в свой аккаунт на компьютере друга?

**Выберите один вариант из списка**

- ☐ компьютер друга такой же безопасный, как ваш собственный, поэтому можно ничего не предпринимать
- ☐ попросить друга отвернуться или закрыть глаза, когда вы вводите пароль
- ☐ не нажимать галочку «Запомнить пароль», а также почистить историю после завершения сессии, или включить инкогнито режим браузера

Правильный ответ: не нажимать галочку «Запомнить пароль», а также почистить историю после завершения сессии, или включить режим браузера

← К вопросам

Вопрос 10:

Как узнать, что сайт, на который вы переходите, защищен?

**Выберите один вариант из списка**

- ☐ ссылка на сайт начинается с http
- ☐ ссылка на сайт начинается с https
- ☐ ссылка на сайт начинается с www

Правильный ответ: ссылка на сайт начинается с https

← К вопросам

## Вопрос 11:

Что нужно мошенникам, чтобы выманивать деньги у обычных пользователей?

Выберите один вариант из списка

- ☐ достаточно простой хитрости;
- ☐ хакерские программы;
- ☐ продвинутые устройства взлома.

Правильный ответ: достаточно простой хитрости ++++++ нажми еще раз!

+ 3 балла за приведенные примеры

← К вопросам

Вопрос 12: Какой платёжный пароль самый надёжный?

**Выберите один вариант из списка**

- ☐ постоянный, его трудно забыть;
- ☐ одноразовый, он действует очень недолго, и его бессмысленно красть;
- ☐ длинный, он состоит из большого количества цифр и букв, и его сложнее подобрать.

Правильный ответ: одноразовый, он действует очень недолго, и его бессмысленно красть

← К вопросам

Вопрос 13:

Кому можно сообщать свой платёжный пароль или код подтверждения по телефону?

Выберите один вариант из списка

- ☐ сотруднику службы безопасности банка или платёжного сервиса;
- ☐ близкому человеку;
- ☐ никому и ни при каких обстоятельствах.

Правильный ответ: никому и ни при каких обстоятельствах

← К вопросам

Вопрос 14: Как поступить, если вы получили сообщение в соцсети от друга, который просит денег взаймы?

**Выберите один вариант из списка**

- ☐ перевести ему деньги;
- ☐ переслать сообщение кому-нибудь ещё, кто сможет дать в долг;
- ☐ проверить друга — спросить, например, как зовут учителя физкультуры в вашей школе.

Правильный ответ: проверить друга — спросить, например, как зовут учителя физкультуры в вашей школе

← К вопросам

### Вопрос 15:

Вам прислали письмо с сообщением о крупном выигрыше в лотерею, но чтобы получить приз, нужно заплатить небольшой взнос. Как вы поступите?

Выберите один вариант из списка

- ☐ заплатите;
- ☐ вступите в переписку, чтобы узнать подробности;
- ☐ пометите письмо как спам и удалите его.

Правильный ответ: пометите письмо как спам и удалите его

← К вопросам

Вопрос 16: Как уберечься от действий мошенников при поисках работы в интернете?

**Выберите один вариант из списка**

- ☐ искать работу только на популярных сайтах (Яндекс.Работа, Rabota.ru, HeadHunter, SuperJob);
- ☐ не откликаться на вакансии работодателей, которые просят что-либо оплатить — будь то учебники и журналы или накладные расходы;
- ☐ игнорировать предложения с неправдоподобно высокой зарплатой.

Правильный ответ: не откликаться на вакансии работодателей, которые просят что-либо оплатить — будь то учебники или накладные расходы

← К вопросам

### Вопрос 17:

Вы нашли объявление, в котором предлагается выполнить лёгкую работу за большое вознаграждение, но заплатят вам лишь после того, как вы всё сделаете. Как правильно поступить в таком случае?

Выберите один вариант из списка

- ☐ срочно откликнуться, пока кто-нибудь вас не опередил;
- ☐ связаться с работодателем и согласиться на работу при условии, что он пришлёт вам письмо, в котором гарантирует оплату;
- ☐ не откликаться на вакансию.

Правильный ответ: не откликаться на вакансию ++++++ нажми еще раз!

+ подарок 3 балла за правильный ответ!!! Ура!!!

← К вопросам

Вопрос 18: В соцсети незнакомый человек попросил вас перевести деньги на электронный кошелёк — его собаке срочно нужна дорогая операция. Как вы поступите?

### Выберите один вариант из списка

- ☐ прежде чем что-либо предпринять, проверите номер кошелька в интернете — возможно, на него принимают и другие переводы, например, платежи за дешёвые авиабилеты или какие-нибудь услуги;
- ☐ не станете переводить деньги, но поделитесь объявлением на своей странице, чтобы смогли помочь другие;
- ☐ как можно скорее сделаете пожертвование, так как операция срочная.

Правильный ответ: прежде чем что-либо предпринять, проверите номер кошелька в интернете — возможно, на него принимают и другие переводы, например, за дешевые авиабилеты или какие-нибудь услуги

← К вопросам

Вопрос 19: Какую информацию о банковской карточке ни в коем случае нельзя сообщать другим людям?

Выберите один вариант из списка

- ☐ имя владельца;
- ☐ пин-код и CVV;
- ☐ срок действия.

Правильный ответ: пин-код и CVV ++++++ нажми еще раз!

+ 10 баллов за расшифровку CVV

← К вопросам

## Вопрос 20:

Почему из кошелька, к которому привязана карта, платить безопаснее, чем напрямую с карты?

**Выберите один вариант из списка**

- ☐ в отличие от банковской карты кошелёк защищён платёжным паролем;
- ☐ при оплате из кошелька не приходится указывать на сайтах данные карты, ведь она уже привязана к кошельку;
- ☐ платёжный пароль для кошелька можно изменить в любой момент, а пин-код карты — гораздо сложнее.

Правильный ответ: при оплате из кошелька не приходится указывать на сайтах данные карты, ведь она уже привязана к кошельку

К вопросам

**«Сегодня основы кибербезопасности важно изучать прежде, чем начинать пользоваться компьютером. И для цифрового поколения, которое даже конструкторы собирает онлайн, важно понимать возможную опасность онлайн-сообщений от незнакомцев или яркой рекламы, открывающей ворота киберпреступникам. Информационная безопасность страны начинается с образования детей в этом направлении. Звучит немного пафосно, но это так»**



Василий Слышкин, директор департамента развития архитектуры и координации информатизации министерства цифрового развития, связи и массовых коммуникаций РФ.

# ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

## ВОЗМОЖНЫЕ СХЕМЫ МОШЕННИЧЕСТВА

- ПОЛУЧЕНИЕ ДОСТУПА К ЛОГИНАМ, ПАРОЛЯМ, БАНКОВСКИМ ДАННЫМ (ФИШИНГ)
- ПОДДЕЛЬНЫЕ МАГАЗИНЫ С ПРОДАЖЕЙ ЧЕРЕЗ ИНТЕРНЕТ
- СБОРЫ СРЕДСТВ ДЛЯ БЛАГОТВОРИТЕЛЬНОСТИ
- САЙТЫ ЗНАКОМСТВ
- ВИРУСНЫЙ КОНТЕНТ
- ИНФОРМАЦИЯ О ЛЕГКОМ ЗАРАБОТКЕ, РАЗМЕЩЕННАЯ В СЕТИ ИНТЕРНЕТ

Каждые 10 секунд в мире совершаются одно интернет-преступление °

## РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ПОИСКУ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

- НЕ СКАЧИВАЙТЕ ИНФОРМАЦИЮ ДЛЯ ВЫПОЛНЕНИЯ РАБОТ ПО УЧЕБЕ С НЕПОВЕРЕННЫХ ИСТОЧНИКОВ
- ИСПОЛЬЗУЙТЕ АВТОРОВ, ЧЕЙ АВТОРИТЕТ НЕ ВЫЗЫВАЕТ СОМНЕНИЙ
- ПОЛЬЗУЙТЕСЬ ОФИЦИАЛЬНЫМИ ЭНЦИКЛОПЕДИЯМИ И СЛОВАРЯМИ
- ПРОВЕРЯЙТЕ ИСПОЛЬЗОВАННУЮ ИНФОРМАЦИЮ. САЙТ ДОЛЖЕН СОДЕРЖАТЬ СВЕДЕНИЯ ОБ АВТОРСТВЕ, КОНТАКТНЫЕ ДАННЫЕ, ССЫЛКИ НА ИСТОЧНИКИ ИНФОРМАЦИИ
- ПРОВЕРЯЙТЕ ССЫЛКИ НА ИСТОЧНИКИ ИНФОРМАЦИИ. НАПРИМЕР, ЕСЛИ ВЫ ВИДИТЕ ФРАЗЫ «ПО ИССЛЕДОВАНИЯМ УЧЕНЫХ», «КАК УТВЕРЖДАЮТ СПЕЦИАЛИСТЫ», СЛЕДУЕТ НАЙТИ ТЕ САМЫЕ ИССЛЕДОВАНИЯ И УТВЕРЖДЕНИЯ СПЕЦИАЛИСТОВ

Нередки случаи увольнения из-за плагиата. Так, в 2018 году за плагиат в диссертации уволен ректор Курганского университета.°

# ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

## ОБЩЕНИЕ С НЕЗНАКОМЦАМИ

- СТАРАЙТЕСЬ НЕ РАЗГОВАРИВАТЬ С НЕЗНАКОМЦАМИ НИ НА УЛИЦЕ, НИ В ИНТЕРНЕТЕ
- НЕ РАССКАЗЫВАЙТЕ ЛИЧНУЮ ИНФОРМАЦИЮ ЧЕЛОВЕКУ, КОТОРОГО НЕ ВИДЕЛИ В ЖИЗНИ
- НЕ РАССКАЗЫВАЙТЕ ТОГО, ЧЕГО СТЫДИТЕСЬ, ЕСЛИ НЕ ХОЧЕШЬ, ЧТОБЫ ЭТО ВСЕ УЗНАЛИ
- ПОМНИТЕ, ЧТО В ИНТЕРНЕТЕ МОЖНО ПРЕДСТАВИТЬСЯ КЕМ УГОДНО
- НАСТОРОЖИТЕСЬ, ЕСЛИ В ИНТЕРНЕТЕ ИНТЕРЕСУЮТСЯ БЛАГОСОСТОЯНИЕМ ТВОЕЙ СЕМЬИ
- НЕ ОПУБЛИКУЙТЕ СВОИ ГЕОЛОКАЦИИ, ЧТОБЫ ЗЛОУМЫШЛЕННИКИ ВАС НЕ НАШЛИ



## ОСКОРБЛЕНИЕ ЛИЧНОСТИ В ИНТЕРНЕТЕ

- НЕ ВСТУПАЙТЕ В ПЕРЕПАЛКУ С ТЕМИ ЛЮДЬМИ, ЦЕЛЮ КОТОРЫХ ЯВЛЯЕТСЯ ОСОЗНАННАЯ ПРОВОКАЦИЯ;
- НЕ СТОИТ РЕАГИРОВАТЬ, ЕСЛИ ВЫ ПОЛУЧИЛИ ОСКОРБИТЕЛЬНОЕ СООБЩЕНИЕ. НЕОБХОДИМО ПРОСТО ПРЕКРАТИТЬ С ЧЕЛОВЕКОМ ОБЩЕНИЕ И ЗАКРЫТЬ СВОЮ СТРАНИЦУ ОТ ПОСТРОННЫХ ЛИЦ.

⚠ Не используйте Интернет для травли других людей. Помните, что это может стать причиной возникновения уголовной ответственности.

# ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

## Родительский контроль от Центра безопасности Google

- Установите правила работы с устройствами и приложениями (Family Link)
- Контролируйте доступ к приложениям с помощью Family Link
- Управление настройками аккаунта ребенка
- Отключайте для устройства доступ к Интернету в определенное время и блокируйте неуместный контент с помощью Google Wifl
- Настройте Google Ассистента в аккаунте вашего ребенка
- Управляйте доступом к веб-страницам с помощью Chrome
- Блокируйте в Google Поиске сайты с контентом для взрослых с помощью фильтров Безопасного поиска <https://safe.google/familylink/familylink>



## Больше информации по интернет-безопасности

## Адрес ресурса

|                                                                                                |                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| МВД РФ «Безопасный интернет - детям»                                                           | <a href="https://xn--b1new.xn--p1ai/Internet_for_kids">https://xn--b1new.xn--p1ai/Internet_for_kids</a>                                                                                                                |
| Региональная общественная организация «Центр Интернет-технологий» (РОЦИТ)                      | <a href="https://rodit.ru/">https://rodit.ru/</a>                                                                                                                                                                      |
| Центр безопасности интернета                                                                   | <a href="https://www.safesurf.eu/">https://www.safesurf.eu/</a>                                                                                                                                                        |
| Фонд развития интернета                                                                        | <a href="http://www.fid.ru/">http://www.fid.ru/</a>                                                                                                                                                                    |
| Центр безопасности Google                                                                      | <a href="https://safety.google/family/parental-supervision/">https://safety.google/family/parental-supervision/</a>                                                                                                    |
| Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт            | <a href="http://4-dell.org/">http://4-dell.org/</a>                                                                                                                                                                    |
| Обеспечение безопасности детей при работе в Интернете, компьютерный портал ozonov.net          | <a href="http://www.ozonov.net/6213">http://www.ozonov.net/6213</a>                                                                                                                                                    |
| «Безопасность детей в Интернете», компания Microsoft                                           | <a href="https://www.fdp.ru/library/book699.pdf">https://www.fdp.ru/library/book699.pdf</a>                                                                                                                            |
| Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций | <a href="https://rkn.gov.ru/">https://rkn.gov.ru/</a>                                                                                                                                                                  |
| Продукты для родительского контроля от производителей антивирусного ПО                         | <a href="https://www.kaspersky.ru/safe-kids">https://www.kaspersky.ru/safe-kids</a><br><a href="https://protection.drweb.ru/components/parental-control/">https://protection.drweb.ru/components/parental-control/</a> |

<https://xn--h1adlhdnlo2c.xn--p1ai/lessons/cybersecurity>

«Приватность в цифровом мире»

<https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-budushhego>

«Безопасность будущего»

«Безопасность будущего»

<https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-v-internete-2018-2019>

«Безопасность в интернете

2018-2019»

2018-2019»

urok@data-economy.ru

УРОК ЦИФРЫ

Все Уроки Навигатор по материалам Личный кабинет

ТРЕТИЙ УРОК СЕЗОНА 2020/2021

# Приватность в цифровом мире

На «Уроке цифры» по теме «Приватность в цифровом мире» ученики смогут познакомиться с основами информационной безопасности и овладеть важным навыком 21 века — умением защищать свои персональные данные.

Дата проведения: 8-22 Февраля 2021

Прохождений: 2 313 178



urok@data-economy.ru

УРОК ЦИФРЫ

Все Уроки

Навигатор по материалам

Личный кабинет

urok@data-economy.ru

УРОК ЦИФРЫ

Все Уроки

Навигатор по материалам

Личный кабинет

## **Квест-игра – «Безопасный Интернет»**

**Цель:** Обеспечение информационной безопасности воспитанников путем привития им навыков ответственного и безопасного поведения в сети Интернет.

### **Задачи:**

Закрепить правила безопасной работы в Сети Интернет;

Развивать логическое мышление, внимание, умение прогнозировать свое поведение в сети Интернет с помощью различных видов заданий;

Воспитывать дисциплинированность при работе в сети; умение работать в сотрудничестве с товарищами в ходе соревнований.

**Оборудование и материалы:** компьютер, проектор, экран, презентация «Безопасный интернет», эмблемы участников викторины: НЕТик и Сетевичок; памятки «Безопасный Интернет», пазлы, ребусы, тематические картинки, рисунки детей, карточки со словами, маршрутные листы,

## **Ход мероприятия**

### **1. Организационный момент**

#### **Слайд 1.**

Как можно чаще улыбайся.

И радость всем свою дари.

С улыбкой лёгкой просыпайся,

От счастья в облаках пари.

Жизнь так прекрасна, улыбайся.

И засмеётся мир с тобой.

Как можно чаще улыбайся.

Встречай улыбкой день любой.

Вот с такого доброго стихотворения я бы хотела начать наше мероприятие.

Улыбнитесь друг другу, настройтесь на дружную и активную работу. Я желаю вам, чтобы работа принесла вам только положительные эмоции!

## **Слайд 2.**

Сегодня у нас с вами необычное мероприятие. Игра-квест!

- Кто знает, что такое квест?

- Итак, что же означает это слово.

- Это приключенческая игра, в которой вы, главные герои, следуете по маршруту и в процессе игры решаете головоломки и задачи.

## **Слайд 3.**

- В Игре участвуют две команды. Давайте поделимся на команды путем жеребьевки. Подойдите ко мне и в мешочке вытяните эмблему: 1 команда – НЕТик и 2-я – Сетевичок.

Представление команд:

### **Команда НЕТик**

НЕТик сплел тут паутинку

Кружевную пелеринку.

В интернете он живет

Этикет преподает.

### **Команда Сетевичок**

Сетевичок – отличный гид!

В сети ему не страшен лабиринт.

- Надеюсь, что мы все сегодня узнаем, участники, какой же команды по праву могут считаться самыми внимательными, самыми сообразительными, самыми эрудированным, какую команду мы можем назвать «Знатоками».

Оценивать ваши результаты будет жюри – присутствующие гости на нашем уроке.

**Слайд 4.** - На столе жюри лежат маршрутные листы команд, на которых будут отображаться результаты каждого тура. (Приложение 1)

## **2. Основной этап.**

-Итак, возвращаемся к нашей Игре.

- Тему квеста я вам намеренно не сообщаю. Вы ее отгадаете сами. А чтобы отгадать, вам понадобятся подсказки, которые вы получите, пройдя первый этап игры.

- Итак, начинаем наш КВЕСТ.

### **Слайд 5. 1 тур путешествия «ПАЗЛ» (Приложение 2)**

На ваших столах лежат пазлы, вам нужно собрать из них картинку. Кто соберет быстрее ПАЗЛ. (команда, собравшая пазл первой - 5 б, 2 команда - 3 б)

Внимательно рассмотрите получившуюся картинку. Это подсказка к теме квеста.

### **Слайд 6. А вот вторая подсказка. Отгадайте загадку:**

Есть такая сеть на свете

Ею рыбу не поймать.

В неё входят даже дети,

Чтоб общаться, иль играть.

Информацию черпают,

И чего здесь только нет!

Как же сеть ту называют?

Ну, конечно ж... (Интернет)

### **Слайд 7. Сообщение темы мероприятия.**

- Итак, какая же тема сегодняшнего квеста? Правильно тема нашего квеста – «Безопасный Интернет».

### **Слайд 8. 2 тур – «ВОЛШЕБНЫЕ РЕБУСЫ»**

- Нужно отгадать ребусы по теме квеста. Один решенный ребус = 1 баллу.

(Приложение 3)

### **Слайд 9. 3 тур - Игра «Да» или «Нет»**

Давайте с вами поиграем. Я буду задавать вопросы, а вы будете отвечать только да или нет. Если ваш ответ да, то вы поднимаете правую руку, если ваш ответ нет, то поднимаете левую руку. Поняли? (подняли правую руку).

Встаём. Приготовились.

ИГРА:

1. Помогает ли интернет в нашей жизни? (Да)
2. Дает нам интернет новые знания? (Да)
3. Можем ли мы получить эти знания на разных сайтах? (Да)
4. Все ли сайты в интернете безопасны? (Нет)
5. Можно ли использовать сеть Интернет без всяких опасений? (Нет)
6. Может ли общение в социальных сетях принести вам какой-нибудь вред? (Да)

### **Слайд 10. 4 тур – «ПОМОГИ ЧЕЛОВЕЧКУ» (Приложение 4)**

- Давайте теперь ответим на вопрос человечка и поможем ему разобраться, чего нужно опасаться при работе в Интернете. Напишите справа от человечка названия интернет-угроз. Чем больше правильных ответов вы дадите, тем больше баллов заработаете. Один правильный ответ = 1 баллу.

- Итак, правильные ответы. Этому человечку и нам с вами надо опасаться при работе с Интернетом вирусов, мошенников, незнакомых людей, незнакомых сайтов...

### **Слайд 11. 5 тур – «ПРАВИЛА» (Приложение 5)**

- Что же нужно делать, чтобы себя защитить? Чтобы это узнать, давайте выполним следующее задание. Каждая команда называет по очереди верное правило, которое начинается со слов “Я никогда не буду...” или “Я всегда буду...”, а продолжение написано на частях пазла.

- Итак, ребята, соблюдайте эти правила и вы будете работать в безопасном Интернете!

| <b>Я никогда не буду...</b>                         | <b>Я всегда буду...</b>                   |
|-----------------------------------------------------|-------------------------------------------|
| Выставлять свое настоящее имя,<br>адрес, телефон    | Рассказывать родителям о проблемах в сети |
| Открывать подозрительные сообщения                  | Хранить свой пароль в тайне               |
| Участвовать в платных играх, конкурсах,<br>лотереях | Обновлять антивирусную программу          |
| Обижать других в социальных сетях                   | Покидать нехорошие веб-сайты              |
| Общаться в сети с незнакомыми людьми                | Вести себя в социальных сетях вежливо     |
| Открывать и пересылать<br>«письма счастья»          | Скрывать информацию о себе                |

### **Слайд 12. 6 тур – «СИТУАЦИИ ИЗ КОНВЕРТА»**

- Ко мне по электронной почте обратились ребята с криком о помощи.
- В конверте изложены ситуации, в которых ребята не могут разобраться. Надеюсь, мы поможем им.
- За каждый правильный ответ – 1 балл.

(УЧИТЕЛЬ ЗАГЛЯДЫВАЕТ В КОНВЕРТ И ИЗВЛЕКАЕТ КАРТОЧКИ, ЧИТАЕТ ДЕТЯМ).

**1.** ДИМА зашел на незнакомый ему сайт. Вдруг на экране компьютера появились непонятные ДИМЕ сообщения. Что ДИМЕ предпринять?

- А. Заккрыть сайт
- Б. Обратиться к родителям за помощью
- В. Самому устранить неисправность

(Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.)

**2.** СВЕТА создала себе электронный ящик. Теперь она может обмениваться сообщениями со своими друзьями. Сегодня на адрес её электронной почты пришло сообщение: файл с игрой от неизвестного пользователя. Как поступить СВЕТЕ?

- А. Скачать файл, и начать играть.
- Б. Не открывать файл.
- В. Отправить файл своим друзьям.

(Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Убедись, что на твоём компьютере установлено антивирусное программное обеспечение. Помни о том, что эти программы должны своевременно обновляться.)

**3.** ДИМА познакомился в Интернете с учеником 8 класса Иваном. Иван не учится с ДИМОЙ в одной школе, и вообще Дима его ни разу не видел. Однажды Иван пригласил ДИМУ встретиться с ним в парке. Что делать ДИМЕ?

А. Пойти на встречу.

Б. Пойти на встречу вместе с мамой или папой.

В. Не ходить на встречу.

(Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.)

**4.** Новый друг ДИМЫ, с которым он познакомился вчера в Интернете, Иван попросил ДИМУ срочно сообщить ему такую информацию: номер телефона, домашний адрес, кем работают родители ДИМЫ. ДИМА должен:

А. Сообщить Ивану нужные сведения.

Б. Не сообщать в Интернете, а сообщить при встрече.

В. Посоветоваться с родителями.

(Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!)

**5.** СВЕТА решила опубликовать в Интернете свою фотографию и фотографии своих одноклассников. Можно ли ей это сделать?

А. Нет, нельзя.

Б. Можно, с согласия одноклассников.

В. Можно, согласие одноклассников не обязательно.

**6.ДИМЕ** купили компьютер. Он теперь целый день проводит за компьютером. Через несколько дней у него стали слезиться глаза, появились боли в руках. Что делать ДИМЕ?

А. Продолжать проводить время за компьютером.

Б. Больше никогда не работать на компьютере.

Г. Соблюдать правила работы на компьютере:

Расстояние от глаз до экрана компьютера должно быть не менее 50 см.

Одновременно за компьютером должен заниматься один ребенок.

Продолжительность одного занятия – не более 60 минут.

После 10–15 минут непрерывных занятий за ПК необходимо сделать перерыв для проведения физкультминутки и гимнастики для глаз.

Продолжительное сидение за компьютером может привести к перенапряжению нервной системы

СПАСИБО ВАМ, РЕБЯТА! НАДЕЮСЬ, МЫ ПОМОГЛИ ДИМЕ И СВЕТЕ.

### **Слайд 13.**

- В социальной сети «ВКонтакте» есть специальная группа, к которой вы можете присоединиться. Называется она – БЕЗОПАСНОСТЬ.

### **Слайд 14. Несколько шокирующих фактов о социальных сетях**

- Сейчас, пока жюри подводит итоги, девочки познакомят нас с интересной информацией. Я надеюсь, что услышав её, вы сделаете для себя определённые выводы.

1. Приблизительно пятнадцатью процентами пользователей социальные сети применяются для организации слежки. Это большей частью практикуется спецслужбами.
2. Среди пользователей соц.сетей **37%** публикуют в них малоинтересные сведения о собственной личной жизни.
3. В соответствии со статистикой количество преступлений, направленных на несовершеннолетних, выросло из-за соц.сетей в **26** раз.
4. Социальные службы используют для вербовки своих агентов не только спецслужбы, но и различные группировки, в том числе террористической направленности.
5. Социальные сети сужают кругозор человека: он становится зависим от пустых и ненужных сообщений.
6. Чрезмерная увлеченность соц.сетями, по данным исследований, ведет к снижению иммунитета, сердечно-сосудистым болезням и другим заболеваниям.
7. В соц.сетях знакомится каждая пятая семья в мире.
8. Средний пользователь посещает аккаунт дважды в день.
9. У среднего пользователя друзьями числится 195 человек.
10. К 2010 году доступ к соц.сетям имело уже 96% населения всей планеты.
11. Наиболее активна Интернет-аудитория в России: средний пользователь проводит в нем 6 часов в неделю, просматривая 1307 Интернет-страниц.
12. 80% компаний мира подбирают сотрудников с помощью соц.сетей.
13. Популярные соц.сервисы продолжают хранить удаленные пользователями изображения.
14. По числу пользователей лидирует Facebook – 1 миллиард пользователей.

15. В сети популярность социальных сетей по результатам проведенного опроса составила: Одноклассники - 73%, Вконтакте - 62%, Facebook - 18%, Twitter - 9% и 1% не знает о сетях ничего.

16. Ежедневно в социальных сетях дети проводят: от 7 до 14 часов – 23%, 14-21 час – 57% и больше 21 часа – 20%.

17. Каждый пятый ребенок из семи дней недели один тратит на соц.сеть.

### **Слайд 15. Подведение итогов**

Сейчас мы с вами подведём мини-итог нашей работы.

Мы с ребятами в игре

С толком занимались.

Безопасность в интернете

Изучить старались.

В интернете дружат с тем,

Кто на форуме сумел

Репутацию создать –

Друга, словом поддержать

Алексей зашёл на сайт,

Другу стал письмо писать.

По ошибке – в каждом слове.

Насмешил народу – море.

Кто грубит в эфире – скверно

Поступает он не верно.

«Троллями» таких зовут,

Дружбу с ними не ведут.

Отвечать на грубость «троллей» -

Ничего глупей, нет более.

Игнорируйте таких –

Покидайте сайты их.

С интернетом водим дружбу –

Никогда не подведёт.

Предоставит всё, что нужно,

Даже плату не возьмёт.

### **Рефлексия**

- Вот и подошла к концу наша Игра-квест.

- Какова была тема нашего мероприятия?

- Верно, “Безопасный Интернет”.

- Что вы запомнили?

- Что полезного Вы узнали?

Ребята прошу Вас оценить нашу игру, как Вы оцениваете посты в социальных сетях. Ставьте лайк, если Вам понравилось и дизлайк если нет.

Итак, итоги игры (озвучиваются результаты). Спасибо вам, ребята, за отличную игру!

- Я вам вручаю памятки, которые вам помогут безопасно покорять Сеть Интернет. (Приложение 6)

Приложение 1

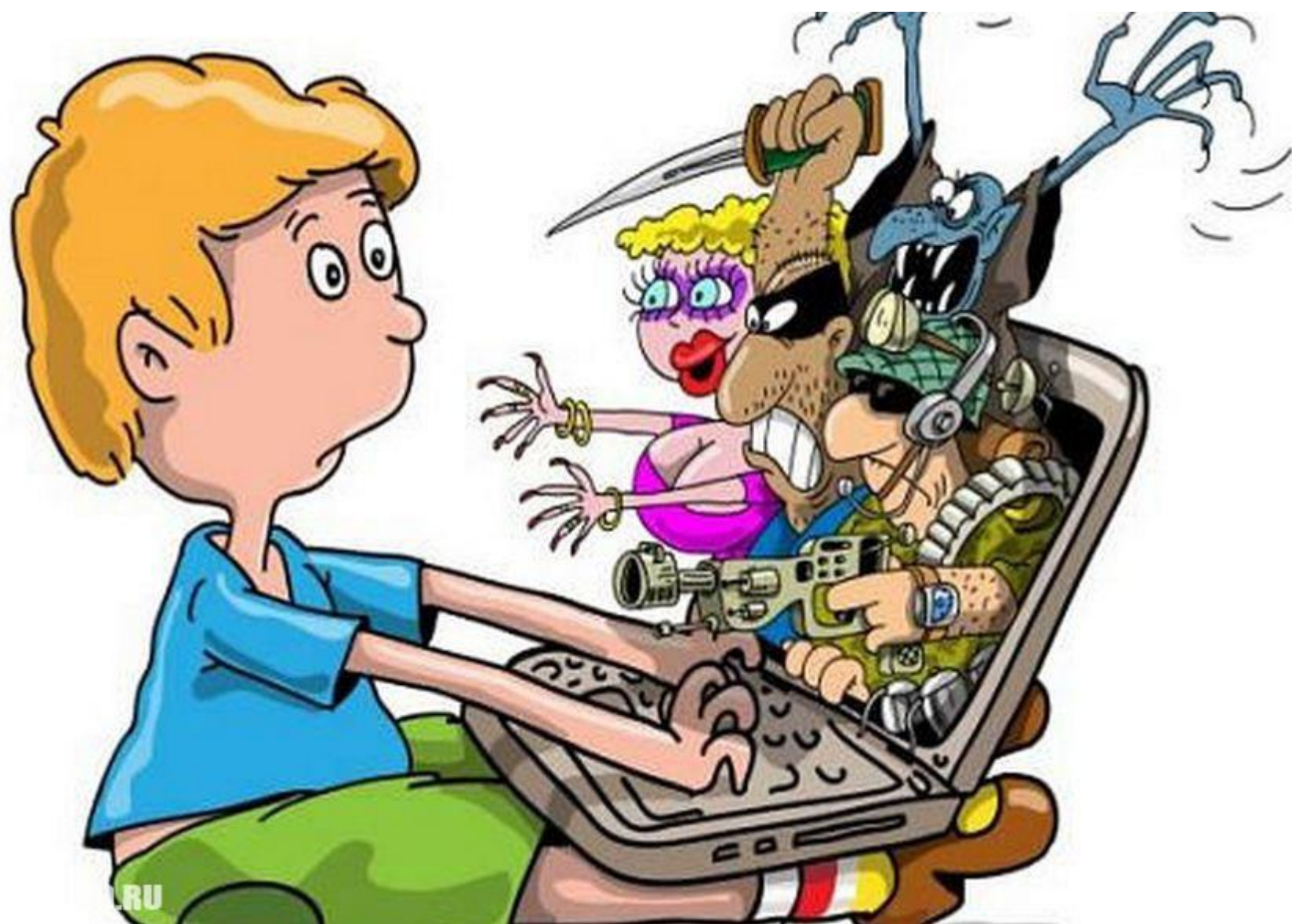
### Маршрутный лист

| Станция              | Баллы |
|----------------------|-------|
| «Пазл»               |       |
| «Волшебные ребусы»   |       |
| «Да или Нет»         |       |
| «Помогите человечку» |       |
| «Правила»            |       |

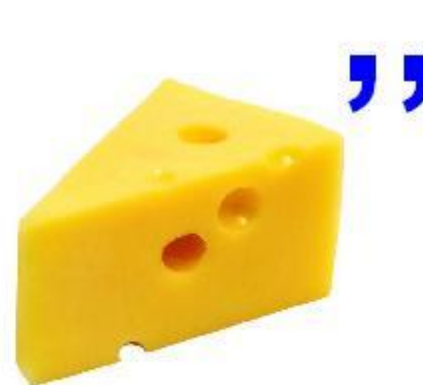
|                        |  |
|------------------------|--|
| «Ситуация из конверта» |  |
| <b>ИТОГО:</b>          |  |

Приложение 2

Пазл



Волшебные ребусы



вирус

”1



”



интернет



компьютер

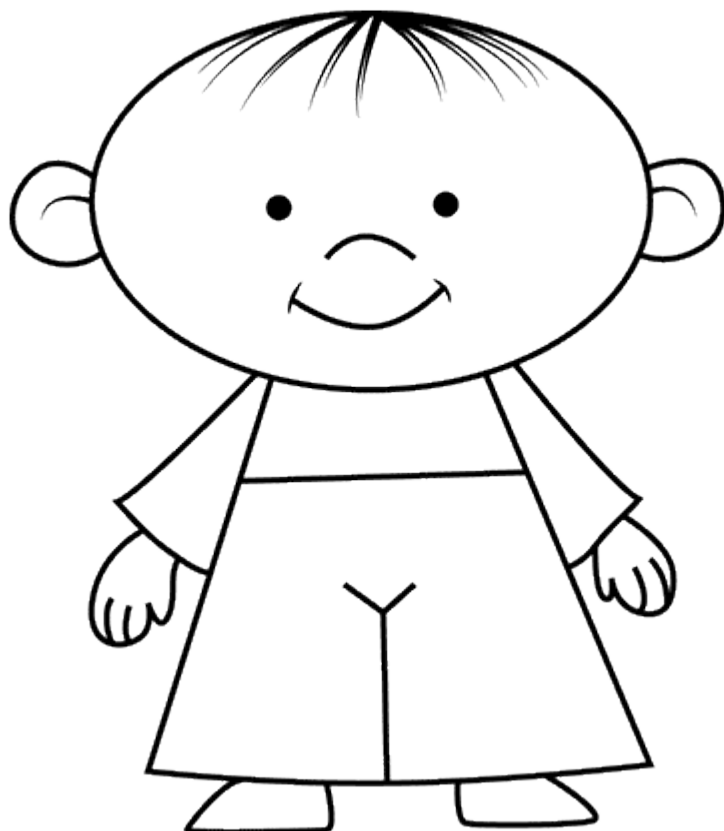


 1 = Н



безопасность

Помоги человечку





П

равила

# Правила безопасности детей в Интернете.

