

3. КИБЕРДЕЛИНКВЕНТНОЕ ПОВЕДЕНИЕ

ДЕЛИНКВЕНТНОЕ ПОВЕДЕНИЕ – это поведение, при котором несовершеннолетним **нарушаются нормы права**, но:



за ним **не следует уголовное наказание** в силу

- либо недостижения ребенком или подростком возраста уголовной ответственности,
- либо незначительности правонарушения.



за ним **следует реальное уголовное наказание**

- если подросток достиг возраста уголовной ответственности и совершил серьезное преступление.

КИБЕРДЕЛИНКВЕНТНОЕ ПОВЕДЕНИЕ — это действия, нарушающие нормы Уголовного кодекса, в ходе которых использовались цифровые технологии и электронные устройства.

ФАКТОРЫ РИСКА, УЯЗВИМОСТЬ И ПОТЕНЦИАЛЬНЫЕ ПРИЗНАКИ



Индивидуальные факторы риска и уязвимость

- ведомость, внушаемость, неспособность сопротивляться вредным влияниям,
- оправдание правонарушений, отрицательное отношение к закону,
- сниженная критичность к своему поведению, непонимание происходящего,
- выраженные эмоциональные особенности (холодность по отношению к другим, сниженная способность к сочувствию, частые колебания настроения, проявления гнева, злости, обидчивости, скрытности, а также чувства одиночества, непонимания другими),
- повышенная возбудимость, импульсивность, беспокойная агрессивность и раздражительность, неумение контролировать себя,
- желание обратить на себя внимание или повышенная общительность,
- невысокие познавательные возможности,
- употребление психоактивных веществ,
- стремление получить сильные впечатления, поиск авантюрных удовольствий, героизация и др.

Социальные факторы риска

- непоследовательные стратегии воспитания, вседозволенность либо заброшенность,
- излишний или недостаточный контроль, авторитарность со стороны взрослых,
- плохие взаимоотношения с близкими, опыт физического или эмоционального насилия,
- недостаток знаний у взрослых о возрастных особенностях детей, способах управления трудными педагогическими ситуациями,
- конфликты в школе, пренебрежение со стороны сверстников,
- отрицательная оценка способностей ребенка взрослыми,
- окружение ребенка или подростка состоит в основном из ребят или взрослых с похожими поведенческими проблемами,
- неорганизованность детского отдыха и досуга,
- примеры преступных действий, насилия, жестокости, безнаказанности, которые наблюдает ребенок в своем ближайшем социальном окружении, продукции СМИ или медиаконтенте в Интернете и др.

Потенциальные признаки киберделинквентного поведения

Поведенческие признаки

- резкие изменения в поведении, настроении, общении с близкими,
- скрытность в отношении онлайн-друзей, виртуальных контактов, своих онлайн и/или офлайн занятий,
- частое ночное использование цифровых устройств (телефона, планшета или персонального компьютера), несмотря на усталость и недосып,
- повышенное внимание к секретности своих цифровых устройств,
- социальная изоляция, уход от реального общения в виртуальное пространство,
- агрессивная реакция на попытки родителей (законных представителей) контролировать онлайн-активность.

Финансовые признаки

- активное использование криптокошельков, чужих банковских карт,
- появление собственных денежных средств в объемах, значительно превышающих карманные деньги,
- неожиданные денежные переводы (в т.ч. крупные) от неизвестных лиц,
- частое получение посылок с неизвестным содержимым,
- попытки обналичивания денег через терминалы без объяснения причин,
- интерес к схемам быстрого заработка в Интернете,
- обсуждение инвестиций и криптовалют со сверстниками или неизвестными лицами,
- демонстрация дорогостоящих вещей без объяснения источника средств.

Технические признаки

- необычные списания с банковских счетов родителей без объяснений,
- активное использование новых малоизвестных мессенджеров и/или средств анонимизации,
- установка программ для шифрования данных и скрытия файлов,
- создание множества аккаунтов в социальных сетях с разными данными,
- использование специфического сленга и криптографических терминов,
- появление второго запасного телефона и/или СИМ-карты.

Психологические признаки

- повышенная тревожность и/или раздражительность при упоминании Интернета и цифровых устройств,
- манипулятивное поведение для получения доступа к деньгам,
- импульсивные покупки в Интернете без согласования с родителями,
- чрезмерная увлеченность онлайн-играми с возможностью микротранзакций.

ФОРМЫ КИБЕРДЕЛИНКВЕНТНОГО ПОВЕДЕНИЯ — онлайн форма или смешанная форма (может проявляться не только онлайн, но и офлайн либо реализуется офлайн, но организация осуществляется в сети Интернет).

ВАЖНО в настоящее время не все виды киберпреступлений четко описаны в уголовном праве. Некоторые из них представлены косвенно (то есть преследуется скорее результат действия, чем сами действия). Поэтому граница того, что можно считать киберпреступлениями размыта. Кроме того, постоянно совершенствуется законодательство, и то, что недавно не входило в киберпреступления, может быть так обозначено.

ПОДВИДЫ КИБЕРДЕЛИНКВЕНТНОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

01

Участие несовершеннолетних в сфере незаконного оборота наркотических веществ посредством Интернета (без элемента склонности к зависимости, но с элементом виктимности)

это форма киберпреступлений, при которой третьи лица используют мобильную связь, цифровые платформы (в том числе различные электронные платежные системы) и анонимные сети для бесконтактной продажи и распространения наркотических и психоактивных веществ. Особую роль играет вовлечение несовершеннолетних в данную деятельность (часто по принципу «сетевого наркомаркетинга»), а также их виктимность, то есть уязвимость перед манипулятивными воздействиями третьих лиц (подростки обладают неустойчивыми психоэмоциональными и волевыми качествами) и подверженность негативным последствиям.

Одним из вариантов вовлечения несовершеннолетних являются сообщения в мессенджерах или социальных сетях с приглашением на работу курьером, при этом сам подросток может не быть осведомленным о содержании доставляемых «заказов». Нередко лица, вовлекающие несовершеннолетних, находят индивидуальный подход к каждому подростку, применяя современные игровые техники: например, «вовлекатели» могут завуалировать преступную деятельность, связанную с наркотиками, в частности, их сбыт, как «квест» либо компьютерную игру, в процессе которых необходимо выполнить определенные действия и получить за это выигрыш, в данном случае денежные средства.



02

Участие в деструктивных (экстремистских, запрещенных) группах

это большой спектр различных манипулятивных способов вовлечения несовершеннолетних к участию в террористической и экстремистской деятельности.



Экстремизм определяется как приверженность крайним мерам и взглядам, радикально отрицающим существующие в обществе нормы и правила через совокупность насильственных проявлений, совершаемых отдельными лицами и специально организованными закрытыми группами и сообществами, через которые организуется противоправная активность.

Для вовлечения несовершеннолетних в противоправную деятельность (в том числе в игровой онлайн форме) может применяться технология манипулятивного воздействия с использованием ботов или специально нанятых пользователей для искусственного управления общественным мнением, создания подставных групп пользователей, размещающих комментарии и пропаганду, популяризирующую и распространяющую деструктивные модели поведения.

03

Диверсионная деятельность

целенаправленная активность, связанная с планированием (в т.ч. онлайн) и/или нанесением ущерба объектам критической инфраструктуры, жизнеобеспечения и общественной безопасности. **Включает:** поиск информации и/или инструкций, распространение и передачу сведений о потенциальных объектах, информационное сопровождение, координацию действий с другими участниками, публикацию призывов или результатов диверсий **через интернет-ресурсы, социальные сети и иные средства электронной коммуникации**. Это крайне опасная форма противоправного поведения, влекущая тяжелые последствия как для общества, так и для подростка.



Совокупность причин: романтизация и/или «нормализация» противоправной деятельности; влияние радикальных групп через интернет-ресурсы, приводящее к появлению новых радикальных увлечений, интереса к материалам и идеологии террористической направленности; манипуляция чувством справедливости; финансовый интерес; стремление к самостоятельности, желание доказать свою значимость, тяга к риску и авантюрам; отсутствие должного контроля со стороны взрослых.

ВАЖНО

формировать у подростков навыки критического анализа информации и безопасного поведения в Интернете, предоставлять информацию о легальных способах трудоустройства несовершеннолетних.

04

Нападения на образовательные организации или иные государственные учреждения

являются (в том числе как следствие участия в деструктивных группах) одним из самых сложных сочетанных видов делинквентного поведения (сочетание признаков агрессивного и суицидального поведения), а также сочетание онлайн (организация) и офлайн (реализация) форм.

ВАЖНО

Представляют собой особые случаи общественно опасных деяний; вызывают повышенную озабоченность сотрудников правоохранительных органов, образования и здравоохранения; часто подобные акты агрессии имеют сходные черты.

Движение в социальных сетях (в виде групп/пабликов/сообществ), посвященное нападениям на образовательные организации, признано террористической организацией и запрещено Верховным судом Российской Федерации.

В ситуации возможного риска нападения обучающимся на образовательную организацию используйте алгоритм действий в 5 памятке [Навигатора профилактики девиантного поведения \(2022\)](#)

ПОДВИДЫ КИБЕРДЕЛИНКВЕНТНОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ



1. Ложный вызов (сваттинг)

форма интернет-троллинга или киберпреступления, при которой в полицию поступает сообщение о ложной угрозе (например, заложенной бомбе, вооруженном преступнике или захвате заложников) по адресу жертвы. Цель — вызвать спецназ или другие силовые структуры к дому жертвы, реализация возможна также с использованием Интернета или IP-телефонии.



2. Кибервыуживание (фишинг)

интернет-мошенничество с целью получения путем подлога адреса организации у пользователей их личных данных (логинов, паролей, банковских и прочих конфиденциальных данных).



3. Кибервзлом (хакерство)

процесс поиска дыр в безопасности компьютерной системы или сети Интернет с целью получения доступа к личной или корпоративной информации.



4. Сексуальное онлайн-вымогательство и/или онлайн-домогательство (грумминг)

вымогательство у сверстников или более младших детей сексуальных изображений, в том числе с помощью угроз или шантажа, а также вовлечение несовершеннолетних в совершение сексуальных действий онлайн.



5. Продажа аккаунтов, СИМ-карт или банковских карт

передача третьим лицам за вознаграждение данных своего аккаунта, или банковской карты, продажа СИМ-карты под влиянием мошенников, которые могут использовать их для противоправной деятельности. Может быть инициирована самим подростком, в связи с чем имеет черты не только киберделинквентного, но и кибервиктимного поведения.



6. Кибердискриминация

ущемление/оскорбление других пользователей по религиозному и/или национальному признаку.

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

При выявлении экстренной опасности для жизни и здоровья окружающих и самого подростка — незамедлительно поставьте в известность руководителя, педагогов и специалистов образовательной организации, сообщите в правоохранительные органы. В случае, если Вы предполагаете, что несовершеннолетний проявляет киберделинквентное поведение, используйте общий алгоритм действий данного Навигатора (памятка 0.4), сообщите администрации образовательной организации, родителям (законным представителям) и при необходимости мотивируйте их на обращение в правоохранительные органы, а также:

- ✳ Отмечайте положительные стороны ребенка, не делая акцент на отрицательных, чтобы не навешивать ярлыки. Старайтесь оценивать не самого ребенка, а его поступки. Избегайте публичного порицания сравнения, выделяя кого-то одного, это может задеть чувства других подростков.
- ✳ В случае возникновения сложной ситуации, решайте проблему, беседуя с ее участниками. Подросток может не сразу открыться, ему нужно время, чтобы довериться. Если его мнение противоречит Вашему, попробуйте построить с ним конструктивный диалог.
- ✳ Обращайте внимание на свои чувства и эмоции. Если Вы злитесь или испытываете другие сильные чувства во время общения с подростком, то переадресуйте решение проблемы другим специалистам (педагогу-психологу или социальному педагогу), чтобы не усугубить ситуацию.
- ✳ В сложных ситуациях привлекайте внимание родителей (законных представителей) к проблеме подростка. Помните, что подросток может скрывать события от родителей. Налаживайте и поддерживайте доверительные отношения с родителями своих подопечных.

В случае риска нападения обучающимся на образовательную организацию и/или делинквентного поведения офлайн также используйте 5 и 6 памятки с алгоритмами действий [Навигатора профилактики девиантного поведения \(2022\)](#)



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

- ✳ Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации (бесплатно, круглосуточно) **8-800-100-12-60#1**
- ✳ Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации (бесплатно, круглосуточно) **8-800-600-31-14**
- ✳ Всероссийский Детский телефон доверия (бесплатно, круглосуточно) **8-800-2000-122**
- ✳ Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

4. КИБЕРВИКТИМНОЕ ПОВЕДЕНИЕ

КИБЕРВИКТИМИЗАЦИЯ ДЕТЕЙ И ПОДРОСТКОВ — это процесс, при котором несовершеннолетние становятся жертвами преступных действий в интернет-пространстве. Ребенок может стать жертвой онлайн и/или телефонной манипуляции, киберагрессии, сексуального онлайн-насилия и эксплуатации, преследования, злоупотребления доверием или введением в заблуждение со стороны посягателя, которые наносят вред его психологическому благополучию, психическому и физическому состоянию. Может происходить со стороны незнакомцев, как взрослых, так и сверстников, и часто сопровождается чувством беспомощности, страха и изоляции.

Дети и подростки легко становятся пострадавшими от противоправных действий в силу возраста, так как зачастую не способны распознавать ситуации риска и оказать посягателю активное сопротивление.

Еще большей уязвимостью отличаются несовершеннолетние, которым свойственно виктимное поведение, т.е. рискованное, необдуманное или чрезмерно доверчивое поведение по отношению к злоумышленникам.



КИБЕРВИКТИМНОЕ ПОВЕДЕНИЕ ДЕТЕЙ И ПОДРОСТКОВ — это действия или реакции несовершеннолетних, которые могут способствовать их субъективной или объективной уязвимости к кибервиктимизации. Оно может включать в себя:



Раскрытие личной информации

Публикация своих данных (имя, адрес, номер телефона, фотографий, аудиосообщений, видеоматериалов) в социальных сетях, на форумах, в сообщениях в мессенджерах, что делает их более доступными для злоумышленников.



Общение с незнакомцами

Участие в онлайн-чатах или социальных сетях, где дети и подростки взаимодействуют с людьми, которых они не знают в реальной жизни, проявление доверия к ним, что может привести к манипуляциям или угрозам.



Игнорирование правил безопасности

Неправильное использование настроек конфиденциальности, отсутствие паролей или использование простых паролей для защиты своих аккаунтов.



Участие в рискованных онлайн-активностях

Принятие участия в опасных челленджах, онлайн-квестах или играх, которые могут привести к физическому или эмоциональному вреду.



Поддержка агрессивного поведения

Участие в кибертравле или агрессивном общении, что может привести к ответной агрессии со стороны других пользователей.

ВАЖНО

родителям (законным представителям) и педагогам необходимо обучать детей и подростков безопасному поведению в Интернете и помогать им развивать навыки критического мышления.

Есть вероятность, что несовершеннолетний стал жертвой, если он:

- находится в подавленном настроении;
- сторонится одноклассников или других детей;
- избегает массовых мероприятий в школе;
- часто болеет, не приходит в образовательную организацию по другим причинам;
- негативно реагирует на сигнал нового сообщения, пришедшего на смартфон;
- отпрашивается с уроков, объясняя это плохим самочувствием;
- проявляет аутоагрессивное поведение (наносит себе порезы, ожоги и т.д.).

Наиболее распространенные переживания жертв сексуального насилия или эксплуатации:

- проявления стрессовых переживаний (например, страхов, тревоги, стыда, ощущения предательства);
- отрицание того, что произошло;
- ре-виктимизация при повторном использовании интимных изображений;
- замкнутость, скрытность, униженность;
- утрата уверенности в собственных суждениях;
- чувство одиночества и/или безнадежности;
- чувство ловушки и невозможности обратиться за помощью;
- сексуализированное поведение.

ФОРМЫ КИБЕРВИКТИМНОГО ПОВЕДЕНИЯ — онлайн форма или смешанная форма (может проявляться не только онлайн, но и офлайн либо реализуется офлайн, но организация осуществляется в сети Интернет).

ПОДВИДЫ КИБЕРВИКТИМНОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

01

Кибертравля (кибербуллинг) и/или иные подвиды киберагрессии

систематическое и целенаправленное негативное воздействие на жертву в социально-сетевой среде с целью причинения психологической травмы.

02

Онлайн и/или телефонное мошенничество

негативное воздействие на жертву с корыстными целями (получение конфиденциальной информации, денежных средств, в некоторых случаях с последующим побуждением жертвы к совершению противоправных действий).

03

Сексуальное онлайн-домогательство (груминг)

форма виртуального общения с ребенком или подростком, в течение которого взрослые люди или более старшие несовершеннолетние стремятся получить интимные материалы, организовать с ним встречу в реальном мире и/или виртуальную сексуальную коммуникацию.

ВАЖНО

наиболее виктимная группа жертв сексуального онлайн-груминга — девочки 11-13 лет. Мальчики также могут становиться жертвами, однако процент потерпевших среди них меньше, но они более восприимчивы, нередко не оказывают сопротивление, а в 14-16 лет могут сами проявлять большую активность.

ПОДВИДЫ КИБЕРВИКТИМНОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ

01

Сексуальное онлайн-вымогательство

вымогательство у детей или подростков сексуальных изображений, в том числе с помощью угроз или шантажа, может быть составной частью процесса сексуального онлайн-домогательства (груминга).

02

Распространение материалов сексуального характера (секстинг)

получение, отправка и пересылка по сети Интернет фото- и видеоматериалов сексуального характера с целью мести, причинения вреда, унижения чести, достоинства и для того, чтобы вызвать последующую травлю жертвы.

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

В ситуации, когда специалист образовательной организации (педагог-психолог, социальный педагог, классный руководитель или педагог) обнаружил признаки, предполагающие возможное сексуальное насилие или злоупотребление в отношении ребенка, необходимо использовать общий алгоритм действий (памятка 0.4) данного Навигатора, а также важно соблюдать последовательность следующих действий:

01

Если у сотрудников образовательной организации возникают подозрения о совершении в отношении ребенка сексуального насилия или злоупотребления, то необходимо обратить внимание на косвенные признаки.



Косвенные признаки: повышенный интерес к вопросам сексуальности, имитация сексуальных действий в игре с другими детьми, демонстрация сведений о половых отношениях, выходящих за пределы возрастной нормы и т.п.

ВАЖНО

к подобным признакам следует относиться с осторожностью, так как их источником могут быть также обстоятельства, не имеющие характера сексуального насилия и злоупотребления.

02

При обнаружении или выявлении признаков следует собрать дополнительную информацию о ребенке и его семье и постараться выяснить, чем обусловлены подобные проявления.

03

Если со временем они сохраняются, то специалисту рекомендуется поговорить с ребенком и спросить его об источниках его знаний и привычек, а также о характере действий в отношении него окружающих.

04

Если в ходе первичной беседы ребенок отрицает какие-либо действия сексуального характера со стороны кого-либо из взрослых или сверстников, то следует продолжить наблюдение за ребенком и его семьей.

05

В случае, если в беседе со специалистом ребенок указывает на факты сексуального насилия или злоупотребления внутри или вне семьи, сотрудники образовательной организации должны принять меры по защите ребенка в будущем:

- если речь идет о внесемейном сексуальном насилии или злоупотреблении, руководитель образовательной организации обязан известить родителей (законных представителей) ребенка. В зависимости от их реагирования на сообщение, родители:



либо сами берут на себя заботу о ребенке и обращаются в правоохранительные органы и в организации, где ребенку может быть оказана медико-психологическая помощь,



либо, в случае их неадекватной реакции, это делает руководитель образовательной организации.

06

Далее следует опираться на алгоритмы, представленные в 6 и 7 памятках [Навигатора профилактики виктимизации детей и подростков \(2024\)](#)



В ситуациях кибертравли (кибербуллинга), иных подвидов киберагрессии также воспользуйтесь общим алгоритмом действий и памяткой 5 [Навигатора профилактики виктимизации детей и подростков \(2024\)](#), а также 4 и 5 памятками данного Навигатора.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

✱ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**

- Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.

✱ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации** – (бесплатно, круглосуточно) **8-800-600-31-14**

- На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.



✱ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации** (бесплатно, круглосуточно) **8-800-100-12-60#1**. Также для обращения доступна короткая комбинация 123

✱ **Горячая линия «Дети Онлайн»** <http://detionline.com/helpline/about>

✱ **ЧАТ-БОТ «Добрыня» (антибуллинг)** <https://t.me/BylingBot>

КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

1. Портал [Растимдетей.рф](#) — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — [бытьродителем.рф](#)

5. КИБЕРВИКТИМНО-ДЕЛИНКВЕНТНОЕ ПОВЕДЕНИЕ

КИБЕРВИКТИМНО-ДЕЛИНКВЕНТНОЕ ПОВЕДЕНИЕ — это смешанный вид поведения, при котором несовершеннолетний становится жертвой телефонных и/или онлайн-мошенников и, в состоянии заблуждения, находясь под их влиянием, совершает противоправные действия агрессивно-насильственного и террористического характера.

Последствия при этом могут быть **крайне серьезными** как для пострадавших от таких действий, так и для самого несовершеннолетнего, который может стать обвиняемым в тяжком уголовном преступлении.

Специалистам следует понимать **характер воздействия на несовершеннолетнего со стороны взрослых злоумышленников**, в результате которого он становится инструментом в их руках.

Мошеннические действия, как правило, включают в себя следующие элементы:



1. Инициация злоумышленниками контакта с несовершеннолетним по телефону или через сообщения в мессенджерах под маской сверстников или авторитетных для подростка лиц.



2. Получение от несовершеннолетнего определенных сведений (например, геолокации).



3. Компрометация: вступление в контакт следующей маски, якобы представляющей правоохранные органы России (МВД, ФСБ), и, вследствие передачи несовершеннолетним этих сведений якобы военному противнику, обвинение его в тяжком преступлении (например, госизмене). Запугивание подростка, угрозы ему самому и его семье.



4. Требование секретности, изоляция несовершеннолетнего от окружающих.



5. Требование денежной компенсации или совершения определенных действий, как правило, деструктивных (например, поджога определенных объектов) якобы «для защиты Родины» или «помощи российским военным».



6. Постоянный контроль и поддержание эмоционального напряжения несовершеннолетнего через сообщения в мессенджерах, аудио- и видеосвязь.



НЕКОТОРЫЕ МЕТОДЫ, КОТОРЫЕ МОГУТ БЫТЬ ИСПОЛЬЗОВАНЫ ПРОТИВ ДЕТЕЙ И ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ

Фишинг

01

это метод, при котором мошенники отправляют поддельные сообщения (например, электронные письма, SMS или сообщения в мессенджерах), которые выглядят как официальные, чтобы заставить жертву раскрыть личные данные, такие как пароли или номера кредитных карт. Пример: мошенник может отправить сообщение, якобы от популярного сервиса, с просьбой подтвердить учетную запись, предоставив личные данные.

Вишинг (голосовой фишинг)

02

это форма фишинга, при которой мошенники используют телефонные звонки для получения личной информации. Пример: мошенник может позвонить ребенку, представившись сотрудником банка, полиции, школы или службы поддержки, и попросить подтвердить личные данные для «проверки безопасности».

Смишинг (SMS-фишинг)

03

это использование текстовых сообщений для обмана жертв с целью получения их личной информации. Пример: мошенник отправляет SMS с сообщением о выигрыше в конкурсе, прося перейти по ссылке и ввести личные данные.

Ловушки с использованием социальных сетей

04

мошенники могут использовать социальные сети для создания фальшивых профилей и взаимодействия с детьми и подростками. Пример: мошенник создает привлекательный профиль и начинает общаться с ребенком, предлагая дружбу или участие в «эксклюзивных» группах, чтобы завоевать доверие.

Манипуляция через эмоции

05

чтобы заставить жертву действовать без размышлений. Пример: мошенник может притвориться, что у него возникли проблемы, и попросить деньги или личные данные, чтобы «получить помощь». Также злоумышленник может убеждать, что ребенок будет героем, если выполнит его «просьбы».

Обман через игры

06

мошенники могут использовать популярные онлайн-игры для манипуляции и обмана. Пример: мошенник может предложить «бесплатные» внутриигровые предметы или валюту в обмен на личные данные или доступ к аккаунту.

Создание ложных угроз

07

чтобы заставить жертву раскрыть информацию или выполнить требования. Пример: мошенник может позвонить и сказать, что у него есть компрометирующая информация о ребенке, и потребовать деньги за ее «недоступность».

Использование доверительных отношений

08

чтобы манипулировать жертвой. Пример: мошенник может представиться другом или знакомым и попросить о помощи, чтобы получить доступ к личной информации.

ВАЖНО

обучение детей и подростков критическому мышлению, осведомленности о рисках и безопасному поведению в Интернете может защитить их от потенциальных угроз.

ПРИЗНАКИ КИБЕРВИКТИМНО-ДЕЛИНКВЕНТНОГО ПОВЕДЕНИЯ

Есть вероятность, что несовершеннолетний стал жертвой телефонных или онлайн-мошенников, если он:

- * Озабочен, теряет интерес к занятиям, к происходящему за исключением его собственного дела.
- * Тревожен, находится в подавленном состоянии, проявляет признаки страха.
- * Сторонится сверстников и взрослых, избегает вопросов, отвечает уклончиво, дает нереалистичные ответы.
- * Интересуется, где можно взять крупные суммы денег, одалживает у знакомых.
- * Закупает приспособления, емкости и материалы для деструктивных действий (горючие материалы, составляющие взрывчатых веществ, канистры и т.п.).

ПРЕВЕНТИВНЫЕ МЕРЫ

Для предупреждения этого типа противоправных действий в отношении несовершеннолетних и со стороны самих несовершеннолетних важна первичная профилактика.

В образовательных организациях необходимо информировать детей, подростков и их родителей (законных представителей) о возможности подобных провокаций и о том, как следует реагировать в подобных случаях:



1. не отвечать на телефонные звонки и сообщения с незнакомых номеров,



2. при появлении сообщений из «правоохранительных органов» сообщать взрослым (родителям, сотрудникам образовательных организаций).

В ситуациях онлайн и/или телефонного мошенничества воспользуйтесь 1 и 2 памятками

Навигатора профилактики виктимизации детей и подростков (2024),

а также 3 и 4 памятками данного Навигатора.



ВАЖНО

следует иметь в виду, что жертвами такого рода манипуляций легче становятся дети и подростки с чертами гиперсоциальности, послушные, исполнительные, впечатлительные, тревожные.

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

При обнаружении признаков вовлеченности несовершеннолетнего в манипулятивное взаимодействие со злоумышленниками помимо общего алгоритма (памятка 0.4) данного Навигатора необходимы следующие действия:

01

Поговорить с ребенком, выяснить причину его необычного состояния и поведения. Учитывая его страх, вызванный запугиванием мошенниками, и возможное нежелание идти на контакт, следует информировать его о возможности манипуляций подобного рода, прояснить для него истинную природу ситуации.

02

Информировать родителей (законных представителей) о ситуации, в которой находится их ребенок.

03

Информировать администрацию образовательной организации, в которой учится ребенок.

04

Сообщить о данной ситуации в правоохранительные органы.

05

Вынести случай на психолого-педагогический консилиум (ППК) с другими специалистами образовательной организации и разработать план помощи семье и одноклассникам ребенка (в случае, если им стала известна информация о данной ситуации). Обратите внимание, что ППК должен носить закрытый характер в силу специфики ситуации и информации.

06

Совместно с другими специалистами образовательной организации разработать программу психолого-педагогических и педагогических мероприятий, направленных на профилактику кибервиктимно-преступного поведения, приступить к реализации этой программы.

ВАЖНО

кибервиктимно-делинквентное поведение несовершеннолетних **нужно отличать** от экстремизма и террористических действий несовершеннолетних, совершаемых также по «заказу» злоумышленников, связь с которыми поддерживается через Интернет, однако по **корыстным мотивам**. В подобных случаях речь может идти о киберделинквентном поведении.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

* **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**

- Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.

Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации – (бесплатно, круглосуточно) **8-800-600-31-14**

- На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.

* **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации** (бесплатно, круглосуточно) **8-800-100-12-60#1**. Также для обращения доступна короткая комбинация 123

* **Горячая линия «Дети Онлайн»** (антибуллинг) **ЧАТ-БОТ «Добрыня»**
<http://detionline.com/helpline/about> <https://t.me/BylingBot>

КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

1. Портал **Растимдетей.рф** — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — **бытьродителем.рф**

6. КИБЕРСАМОПОВРЕЖДАЮЩЕЕ И КИБЕРСУИЦИДАЛЬНОЕ ПОВЕДЕНИЕ

САМОПОВРЕЖДАЮЩЕЕ ПОВЕДЕНИЕ (СЕЛФХАРМ) — это комплекс действий аутоагрессивного характера, нацеленных на причинение физического вреда собственному телу (включает несуицидальное самоповреждающее поведение и суицидальные попытки).

НЕСУИЦИДАЛЬНОЕ САМОПОВРЕЖДАЮЩЕЕ ПОВЕДЕНИЕ — потенциально нелетальный намеренный акт аутоагрессивного поведения, связанный с физическим повреждением собственного тела и не имеющий в своей основе для человека цели собственной смерти.



Некоторые возможные действия:
порезы, расцарапывание, обжигание кожи, удары головой или кулаком о стену и др.

ВАЖНО в киберпространстве такое поведение может иметь смешанный характер — несовершеннолетние могут помещать фото и видеоматериалы о своем реальном самоповреждающем поведении и/или суицидальных действиях, но возможно и моделирование таких действий посредством цифровых технологий, а также сознательное нанесение ущерба своей цифровой личности.



Менее очевидные симптомы:
голодание, переедание, злоупотребление алкоголем или ПАВ, нанесение шрамов и др.

СУИЦИДАЛЬНОЕ ПОВЕДЕНИЕ — это диапазон различных вариантов сочетания суицидальных мыслей и суицидальных действий.

ВАЖНО наиболее уязвимой в отношении самоубийства возрастной группой являются подростки, однако в последние годы отмечается тенденция к снижению возраста первого дебюта.

В развитии суицидального поведения особую роль играют социально-психологическая дезадаптация, суицидальное кризисное состояние, суицидальный риск и пресуицидальный период, то есть период формирования суицидальной активности, границами которого являются момент возникновения суицидальных побуждений и момент осуществления суицидальных действий.



В настоящее время может демонстрироваться в онлайн-среде:
КИБЕРСУИЦИД – формирование и/или реализация суицидальных мыслей посредством разнообразных форм участия в интернет-коммуникации.

Признаки киберсамоповреждающего и киберсуицидального поведения

- Размещение (сохранение на своих интернет-ресурсах, отметка «нравится») материалов о самоповреждениях/суицидальной направленности (хэштеги, картинки, видео, песни и т.д.).
- Комментарии материалов о самоповреждениях/суицидальной направленности, особенно на онлайн-форумах.
- Участие в сообществах на тему самоповреждений/суицидальной направленности (нормализация и героизация такого поведения).
- Опыт киберагрессии (травли и/или социальной изоляции).
- Люди реализуют свою потребность в поиске поддержки; осмыслении своих чувств; понимании того, что их проблема не уникальна.
- Нормализация и положительная оценка суицидального поведения, поиск напарников для совершения суицида и свободное распространение информации о способах самоповреждения, повышение уровня безнадежности.

Особенности поведения несовершеннолетнего, которые могут насторожить

- Устойчивые (в течение более 2-х недель) проявления подавленного настроения, пониженного эмоционального фона (включая чувства безнадежности, одиночества, тревоги), раздражительности.
- Резкое снижение успеваемости, проявление безразличия к учебе и оценкам.
- Любые резкие изменения в привычном поведении (например, стал неряшливым, не хочет разговаривать с друзьями, потерял интерес к тому, чем раньше любил заниматься, пропускает занятия; стал более импульсивным, эмоциональным или замкнутым).
- Прямые или косвенные заявления о желании умереть, или убить себя, или о нежелании продолжать жизнь (даже если педагогу кажется, что эти заявления носят демонстративно-шантажный характер).
- Наличие рискованного, агрессивного поведения, фактов употребления ПАВ, алкоголя.
- Наличие фактов ухода из дома.

ФОРМЫ КИБЕРСАМОПОВРЕЖДАЮЩЕГО И КИБЕРСУИЦИДАЛЬНОГО ПОВЕДЕНИЯ — онлайн форма или смешанная форма (проявляется не только онлайн, но и офлайн или наоборот).

ПОДВИДЫ КИБЕРСАМОПОВРЕЖДАЮЩЕГО И КИБЕРСУИЦИДАЛЬНОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

- 01 Киберсамоповреждение (селфхарм)**
в сети Интернет проявляется в виде публикации контента, связанного с данной тематикой в своем аккаунте, паблике или канале, или размещении своего контента (фотографий, видео; наиболее частая форма — порезы кожи и расцарапывание кожи при помощи острых предметов) в сетевых сообществах социальных сетей.

02 Киберсамоубийство
действия, направленные на групповое или индивидуальное лишение себя жизни, которые совершаются в результате и/или посредством использования интернет-ресурсов.

03 Информационный киберсуицид
самоубийство с применением знаний, почерпнутых из Интернета.

04 Онлайн-киберсуицид
самоубийство в реальном времени, перед веб-камерой.
- 05 Парный онлайн-суицид**
самоубийство, при котором инициатор ищет себе партнера в сети Интернет.

06 Коммуникативный киберсуицид (флешмоб-суицид)
объединение ранее незнакомых между собой людей с целью группового онлайн-самоубийства на основе виртуального договора.

07 Аддиктивный киберсуицид
аутоагрессивные действия, спровоцированные интернет-зависимостью.



ПОДВИДЫ КИБЕРСАМОПОВРЕЖДАЮЩЕГО И КИБЕРСУИЦИДАЛЬНОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ

01

Цифровое самоповреждение

направленное на самого себя влияние негативного онлайн-контента, цель которого заключается в том, чтобы вызвать у себя психологический дистресс или косвенно сообщить окружающим о своих психологических проблемах. Может включать в себя любой способ преднамеренного поиска и публикации оскорбительного контента о себе, например, создание негативного блога о себе или публикацию оскорбительных комментариев к собственным фото или видео анонимно, либо из ложного аккаунта, созданного специально для этой цели, известного как аккаунт-призрак.



02

Ведение ауточата с суицидальной направленностью

создание онлайн заметок или онлайн дневника с имитацией общения, где потенциальный суицидент ведет внутренний диалог о смерти и/или планировании самоубийства, оставляя цифровой след. Может проявляться в двух вариантах:

- 1. ведение переписки в чате с самим собой без присутствия других лиц;
- 2. организация в мессенджере или социальной сети закрытого канала/паблика, в который никто не может зайти, и ведение в нем диалога с самим собой.



Такой внутренний диалог может являться выражением эгоцентрической речи, с помощью которой подросток пытается овладеть своим поведением, но в ходе которого происходит сильное эмоциональное самонакручивание, самоубеждение, постоянное прокручивание в голове негативных, депрессивных или тревожных мыслей и воспоминаний (то есть руминация).

03

Участие в деструктивных группах как проявлении аутоагрессивного поведения:

- посвященных суицидальной тематике (например, «группы смерти») или самоповреждениям. Нередко подобные группы ведут «кураторы», наполняющие группы подобным медиаконтентом и организовывающие опасные онлайн-квесты;
- посвященных диетам. Подобные группы часто ведутся людьми, далекими от медицины, и следование их советам приводит к ущербу для жизни и здоровья.

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

В случае, если Вы:

- знаете, что несовершеннолетний проявляет киберсамоповреждающее или киберсуицидальное поведение,
- обнаружили у ребенка или подростка признаки наличия депрессивного состояния, факты нанесения себе физического вреда, суицидальные мысли **нужно незамедлительно** (сохраняя конфиденциальность по отношению к третьим лицам и этические нормы) воспользоваться общим алгоритмом действий (памятка 0.4), а также:

01

сообщить родителям (законным представителям) ребенка о своих наблюдениях с целью мотивирования семьи на обращение за помощью к профильным специалистам;

02

сообщить педагогу-психологу (при отсутствии – социальному педагогу, заместителю директора по воспитательной работе) о своих наблюдениях с целью (при необходимости) принятия оперативных мер для оказания экстренной помощи обучающемуся;

03

сообщить администрации образовательной организации о сложившейся ситуации с целью принятия управленческих решений по привлечению специалистов для оказания помощи, а также для составления плана психолого-педагогического сопровождения обучающегося;

- подозреваете влияние на ребенка **третьих лиц через Интернет**, то в этом случае необходимо **сообщить** в правоохранительные органы.

ВАЖНО

доведение до самоубийства, склонение к совершению самоубийства или содействие совершению самоубийства, а также организация деятельности, направленной на побуждение к совершению самоубийства являются преступлениями в соответствии со ст. 110, ст. 110.1, ст. 110.2 Уголовного кодекса РФ.

В случае смешанной формы киберсамоповреждающего и киберсуицидального поведения также используйте 4 памятку

[Навигатора профилактики девиантного поведения \(2022\)](#)



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

- Всероссийский Детский телефон доверия (бесплатно, круглосуточно) **8-800-2000-122**

• Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.

- Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации – (бесплатно, круглосуточно) **8-800-600-31-14**

• На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.

- Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации (бесплатно, круглосуточно) **8-800-100-12-60#1**. Также для обращения доступна короткая комбинация 123

- Горячая линия «Дети Онлайн» <http://detionline.com/helpline/about>

- ЧАТ-БОТ «Добрыня» (антибуллинг) <https://t.me/BylingBot>

КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

- Портал Растимдетей.рф — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
- Психологический университет для родителей «Быть родителем» — [бытьродителем.рф](#)

7. КИБЕРАДДИКТИВНОЕ ПОВЕДЕНИЕ

КИБЕРАДДИКТИВНОЕ ПОВЕДЕНИЕ — это пристрастие к занятиям, связанным с использованием компьютера (или иного цифрового устройства), приводящее к резкому сокращению всех остальных видов деятельности, ограничению общения с другими людьми.

Есть вероятность, что у несовершеннолетнего могут быть проблемы, если:

- * он предпочитает онлайн-коммуникации (в интернет-пространстве в целом, в играх, в частности), а не живое общение лицом к лицу,
- * у него наблюдается улучшение эмоционального состояния через игровую или другую активность с использованием цифровых технологий,
- * он демонстрирует неконтролируемое регулярное мысленное возвращение в онлайн-пространство (пространство игры или другую активность),
- * он не может оторваться от устройства, бывают трудности планирования своего пребывания в сети (в игре в частности),
- * у него имеются последствия в повседневной жизни (трудности с окружающими людьми, а также сложности в управлении собственной жизнью).

ФОРМЫ КИБЕРАДДИКТИВНОГО ПОВЕДЕНИЯ — онлайн форма (например, сетевые игры или зависимость от социальных сетей) или смешанная форма (может проявляться одновременно в онлайн и офлайн либо проявляется офлайн, но основные действия осуществляются в сети Интернет. Например, игнорирование мобильным).

ПОДВИДЫ КИБЕРАДДИКТИВНОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ

01 Интернет-зависимость

чрезмерное недостаточно контролируемое поведение, связанное с использованием Интернета, вызывающее пагубные последствия и приводящее к снижению качества социального и личного функционирования, а также к нарушениям психического и физического здоровья.



02 Игровая зависимость (гейм-аддикция и гэмблинг)

игровое поведение, осуществляемое посредством сети Интернет:

- * зависимость от видеоигр (гейм-аддикция),
- * зависимость от азартных игр (гэмблинг, лудомания), один из вариантов гэмблинга — беттинг-аддикция или зависимость от ставок на спорт).

Иногда говорят об интернет-зависимости как обобщающем термине, однако игровая зависимость может быть как частью ее, так и отдельным видом зависимости.

ВАЖНО интернет-зависимость — это изменение состояния сознания как следствие особой ценности активности в Интернете и уход от реальности, связанный с проблемами в учебной и иных видах деятельности, а также в межличностных отношениях. Человек может быть зависим от разных технических объектов и видов деятельности, которые реализуются через Интернет.

03 Проблемное использование Интернета

чрезмерная степень использования Интернета, которая может приводить к возникновению психологических, социальных, академических и профессиональных трудностей, а также может включать в себя и другие деструктивные виды использования интернет-технологий (например, кибертравлю).

По другим основаниям среди подвидов кибераддиктивного поведения онлайн формы также выделяют:

04 Зависимость от устройств (гаджетов)

куда входит часто упоминаемая компьютерная зависимость.



05 Одержимость онлайн-новостями (думскроллинг)

зависимость от чтения негативных новостей, когда человек не может остановиться, пропуская через себя все больше и больше информации.

06 Запойный просмотр видеоконтента (бинджвотчинг)

изначально рассматривался просмотр только нескольких серий или всего сезона серийных шоу, однако в последнее время понимание данного феномена расширилось, и исследователи рассматривают не только просмотр телесериалов, но и другого продолжительного видеоконтента.

ПОДВИДЫ КИБЕРАДДИКТИВНОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

01 Игнорирование мобильным (фаббинг)

пренебрежительное отношение к собеседнику, которое выражается в постоянном отвлечении от разговора ради того, чтобы «быстренько заглянуть в телефон».

02 Киберотлынивание (кибербезделье, киберлафинг)

форма использования технических устройств (чаще всего с доступом к Интернету) в личных целях во время учебы (академический киберлафинг) или работы (бизнес-киберлафинг). Это особая форма ухода от скучной работы или вариант прокрастинации, осуществляемый за счет использования информационных технологий.

03 Одержимость покупками (онлайн-шопинг) или листанием онлайн-каталогов (скроллшоппинг).

ВАЖНО

при кибераддиктивном поведении может проявляться абстинентный синдром (синдром отмены) — комплекс психологических и физических симптомов, которые возникают при резком прекращении или значительном сокращении использования Интернета и связанных с ним технологий.

✳ **Психологические симптомы:** при отсутствии доступа к Интернету человек может испытывать повышенную тревожность, нервозность и раздражительность. В некоторых случаях может проявляться пониженное настроение, особенно если Интернет использовался как способ избежать реальных проблем или эмоций. Без доступа к Интернету человек может чувствовать себя скучно и не знать, чем заняться, что может привести к снижению мотивации. Люди могут испытывать трудности с сосредоточением на задачах.

✳ **Физические симптомы:** некоторые люди могут испытывать головные боли, особенно если они привыкли проводить много времени за экраном. Изменения в режиме сна, такие как бессонница или повышенная сонливость, могут быть следствием отмены. Могут возникать симптомы, такие как мышечное напряжение или общее недомогание.

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

В случае, если Вы знаете, что несовершеннолетний проявляет кибераддиктивное поведение используйте общий алгоритм действий (памятка 0.4) данного Навигатора, а также необходимо:

01

Сохранять контакт с ребенком или подростком. Для этого: помните, что авторитарный стиль взаимодействия для подростков неэффективен и даже опасен. Чрезмерные запреты, ограничения свободы и наказания могут спровоцировать у подростка ответную агрессию и заставить погрузиться его еще глубже в аддиктивное поведение. В подростковом возрасте предпочтительной формой взаимодействия является заключение договоренностей. Если ограничение необходимо, не пожалейте времени на объяснение его целесообразности.

02

Способствовать созданию дружеской поддерживающей атмосферы, ориентировать детей и подростков на совместную деятельность и сотрудничество. Всегда внимательно выслушивать жалобы детей, помогая им разобраться в возникшей ситуации.

03

Обращать внимание на ситуации, когда один или несколько детей или подростков явно демонстрируют какой-либо вид кибераддиктивного поведения (чаще всего игры), проведите разъясняющую беседу с ним лично, поговорите с родителями (законными представителями), для дополнительной помощи обратитесь к педагогу-психологу и социальному педагогу.

04

Встречи используйте как место и время поговорить о личных интересах каждого ребенка или подростка, ненавязчиво пропагандируя здоровый образ жизни.

05

Важно поддерживать диалог с ребенком или подростком, оставлять возможность, чтобы при необходимости он мог обратиться к Вам в трудной жизненной ситуации.

06

Способствовать развитию умения у детей и подростков отстаивать свою точку зрения в дискуссиях со взрослыми, это поможет им легче отказаться от зависимости.

В случае сочетания кибераддиктивного поведения с другими видами аддикций также используйте 7 памятку [Навигатора профилактики девиантного поведения \(2022\)](#)



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

✳ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**

- Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.

✳ **Горячая линия «Дети Онлайн»**

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

✳ **ЧАТ-БОТ «Добрыня» (антибуллинг)**

<https://t.me/BylingBot>



✳ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации** (бесплатно, круглосуточно) **8-800-600-31-14**

- На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.

КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

1. Портал [Растимдетей.рф](#) — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — [бытьродителем.рф](#)

8. КИБЕРРИСКОВАННОЕ ПОВЕДЕНИЕ

КИБЕРРИСКОВАННОЕ ПОВЕДЕНИЕ — это реализованное стремление несовершеннолетних к опасной неопределенности с использованием цифровых технологий. Такое поведение связано с возможностью наступления негативных последствий как для их безопасности, так и для их психоэмоционального состояния, несмотря на равную вероятность наступления положительного исхода.

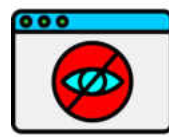
Среди киберрискованных действий можно выделить:

- Общение с незнакомцами**
что может привести к риску киберагрессии, манипуляций, вовлечения в деструктивные сообщества или даже угроз (например, принятие запросов на дружбу от незнакомцев в социальных сетях или участие в чатах с незнакомыми людьми).
- Публикация или отправка в сообщениях личной информации**
что может обуславливать кибервиктимизацию (примеры раскрытия личной информации: публикация фамилии и имени, полной даты рождения, домашнего адреса, номера телефона, номера школы и класса, информации о семье или других идентифицирующих данных).
- Игнорирование настроек конфиденциальности**
в социальных сетях может привести к тому, что личная информация станет доступной для широкой аудитории (например, открытые профили в социальных сетях, где любой может видеть публикации и личные данные).
- Кликание на подозрительные ссылки**
которые ведут на вредоносные сайты или содержат вирусы (например, получение сообщений с подозрительными ссылками от незнакомцев или в результате фишинга).
- Участие в опасных онлайн-играх или онлайн-квестах**
которые могут содержать элементы насилия или рискованные задания в офлайн, и могут быть опасны для здоровья и безопасности.
- Использование ненадежных, недостоверных источников информации**
это может привести к распространению дезинформации или формированию неправильных представлений (например, дети и подростки могут верить в фейковые новости или участвовать в обсуждениях на форумах, где распространяется ложная информация).

Есть вероятность, что у несовершеннолетнего могут быть проблемы, если он:



использует специфический сленг. Следует иметь в виду, что сленг достаточно быстро меняется



стремится скрывать свою онлайн-активность или чрезмерно бравирует этим



принимает участие в группах и форумах, посвященных рискованной тематике (например, «Как быстро заработать» и т.д.)



на страницах в социальных сетях появляются соответствующие фотографии и видео (не обязательно свои)

ФОРМЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ — онлайн форма (хотя в некоторых случаях подготовка может осуществляться офлайн) или смешанная форма (может начинаться в онлайн, переходить в офлайн, а результаты публиковаться в сети Интернет).

ПОДВИДЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

1

Повторы онлайн-трендов

в том числе опасных и/или вирусных с последующей публикацией как подражание современным лидерам мнений (из жизни, видео и т.д.).



2

Просмотр шокирующих материалов (шок-контента)

в различных формах подачи (аудио, видео, текст), основная цель которых оказать сильное влияние на восприятие, вызвать душевные переживания и остаться в памяти как в день ознакомления с такой информацией, так и надолго, заставляя периодически воссоздавать запечатленный образ в сознании.

3

Опасное селфи и/или видео*

несовершеннолетний самостоятельно делает фотоснимок или видеозапись самого себя с помощью камеры мобильного или иного устройства в опасных для жизни условиях обычно с целью дальнейшей публикации в Интернете.

* Часто сочетается с рискованным поведением офлайн, которое может повлечь административную и уголовную ответственность, таким как:



- зацепинг** — способ передвижения, при котором человек цепляется за внешние элементы движущегося транспорта, может включать в себя *трейнсерфинг* (передвижение на крыше поезда), *трейнхоппинг* (запрыгивание на поезд), *фрейтхоп* (передвижение на грузовом поезде), *трейлсерфинг* (ездой между или под вагонами, на хвостовом вагоне или крыше поезда),
- крышолозание (руфинг)** — лазание по крышам высоких строений, небоскребов, многоэтажных жилых домов, а также по радиовышкам,
- диггерство** — незаконное исследование искусственных подземных коммуникаций или сооружений, например, бомбоубежищ, закрытых станций метро, бункеров и др.,
- сталкеринг** — посещение покинутых (заброшенных) объектов и мест, например, оставленных жилых домов, недостроенных зданий и иных мест,
- другие проявления рискованного экстремального досуга.

ПОДВИДЫ КИБЕРРИСКОВАННОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ



1. Маргинальная видеотрансляция (трэш-стриминг)

ведущий за вознаграждение от зрителей выполняет их задания, при этом эфир потенциально пропагандирует насилие и жестокое обращение с людьми и/или животными, унижение человеческого достоинства.



3. Сексуализированная самопрезентация

форма самовыражения, при которой демонстрируется своя сексуальность через различные каналы, такие как социальные сети, мессенджеры или другие онлайн-платформы. Может включать в себя публикацию откровенных фотографий, видео, использование провокационных нарядов или языка, а также активное участие в обсуждениях на сексуальные темы. Данный подвид киберрискованного поведения увеличивает риски эксплуатации, груминга и виктимизации.



2. Рискованный онлайн-заработок

способы получения дохода в Интернете, которые могут быть связаны с высокими финансовыми, юридическими или репутационными рисками. Такие методы часто привлекают людей, обещая быстрые и большие прибыли, но могут привести к потерям или другим негативным последствиям.



4. Просмотр сексуализированных фото- и видеоматериалов (порнографии)

АЛГОРИТМ ДЕЙСТВИЙ СПЕЦИАЛИСТОВ

Что делать, если Вы точно знаете, что у обучающегося киберрискованное поведение:

- 01 Используйте общий алгоритм действий (памятка 0.4) данного Навигатора.
- 02 Проведите индивидуальную беседу с подростком с целью установления мотивации и оценки степени угрозы для его жизни и здоровья.
- 03 Установите связь с родителями (законными представителями) обучающегося. Если они не знают о его увлечениях, аккуратно объясните всю ситуацию, попросите их не ругать ребенка. Выработайте единую стратегию поведения. Возможно, семье нужна дополнительная психологическая и/или социальная помощь.
- 04 Вынесите этот случай на психолого-педагогический консилиум (ППк) с администрацией и другими специалистами образовательной организации (педагогом-психологом, социальным педагогом, другими специалистами). При необходимости иницилируйте Совет профилактики.
- 05 Выработайте индивидуальную траекторию помощи с обязательным привлечением родителей (законных представителей) обучающегося и возможным привлечением различных специалистов.

Основные принципы разговора с обучающимся:

- **до беседы** изучите тот вид деятельности, которым увлекается подросток,
- **во время беседы:**
 - ✳ используйте спокойный доброжелательный тон,
 - ✳ избегайте осуждения, оценивания и нравоучений. Дайте понять, что Вы, в первую очередь, беспокоитесь за его безопасность и не ставите своей целью наказать,
 - ✳ предоставьте подростку возможность высказаться, поделиться своими ощущениями и переживаниями по поводу его увлечений. Это поможет определить мотивацию и на основе этого выстроить план работы с этим подростком и/или его семьей,
 - ✳ убедитесь в том, что подросток полностью осознает, как административные риски, так и опасность для жизни и здоровья. Для этого задавайте открытые вопросы (например, «Как ты считаешь, есть ли какая-то опасность в твоих увлечениях?», «Может ли это причинить кому-то вред? Кому? Какой вред?» и т.д.)

В случае сочетания киберрискованного поведения с другими видами рискованного поведения также используйте 8 памятку [Навигатора профилактики девиантного поведения \(2022\)](#)



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

- ✳ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.
- ✳ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации** (бесплатно, круглосуточно) **8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.

- ✳ **Горячая линия «Дети Онлайн»**
<http://detionline.com/helpline/about>

- ✳ **ЧАТ-БОТ «Добрыня» (антибуллинг)**
<https://t.me/BylingBot>



КУДА МОЖНО НАПРАВИТЬ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

1. Портал [Растимдетей.рф](http://rastimdetey.rf) — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — bytyroditeljem.rf

1. РЕКОМЕНДАЦИИ ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Дети и взрослые используют разные устройства, чтобы общаться и узнавать много нового в Интернете. Но важно пользоваться им очень аккуратно.

Если ты с разрешения родителей во время учебы или отдыха используешь Интернет, следуй правилам, которые описаны ниже. Они помогут тебе быть внимательным и осторожным в онлайн-сети, а также заботиться о себе, своих близких, друзьях и других людях.

1 Используй Интернет только с разрешения родителей и будь осторожен онлайн. Старайся ограничить время, проведенное в Интернете. Делай перерывы, чтобы не переутомляться. И занимайся другими видами деятельности.



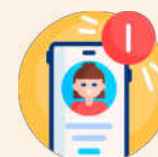
2 Обсуждай с родителями и близкими взрослыми те развлекательные сайты, мессенджеры или игры, в которых хочешь зарегистрироваться или которые используешь.



3 Вместе с родителями настрой в телефоне, на планшете или компьютере конфиденциальность: спрячь свою личную информацию, пусть ее видят только близкие, друзья и учителя.



4 Не публикуй в Интернете личную информацию: не пиши свою фамилию, имя, дату рождения, номер телефона, свой домашний адрес и номер школы. Исключение составляют только чаты с родителями или школьные чаты с учителями.



5 Не выкладывай в Интернете свои фото, видео или голосовые сообщения – ими могут воспользоваться злоумышленники.



6 Если у тебя есть страница или канал в социальных сетях, которые ты ведешь с разрешения родителей, ограничь доступ к своим публикациям для посторонних людей. Попроси родителей помочь тебе настроить их так, чтобы твои посты могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно, учителя).



7 Попроси родителей научить тебя создавать сложные пароли: пароль должен состоять из букв, цифр и специальных символов.



8 Не используй один и тот же пароль для разных приложений. Регулярно меняй пароли. Никогда не делись своими паролями с другими, даже с друзьями, пароль должны знать только родители.



9 Регулярно напоминай родителям обновлять антивирус на твоих устройствах, он защищает от вирусов и нежелательных программ. Но антивирусные программы должны выбирать взрослые.



10 Будь вежлив в Интернете с другими пользователями, если ты общаешься в чатах, например, чате класса.



11 Обсуждай с родителями или учителями ситуации, с которыми ты сталкиваешься в Интернете, и которые тебя тревожат или пугают. Обязательно прекрати общение и расскажи об этом родителям или учителям, если кто-то в Интернете:

- обижает тебя, или ты чувствуешь себя там не так, как хочешь (например, неудобно или неприятно),
- ведет себя странно, расспрашивает о твоей семье или просит сделать что-то плохое или постыдное.



- 12 Не общайся с незнакомыми людьми и не принимай их в друзья,** если у тебя есть мессенджеры или социальные сети. Не принимай от них и не отправляй им личные сообщения. Общайся только на проверенных родителями платформах.
- 13 Если в Интернете случилось что-то плохое,** например, кто-то написал тебе что-то обидное или ты увидел что-то нехорошее в Интернете, сохрани это как картинку или сообщение, чтобы показать близким взрослым.
- 14 Если с разрешения родителей ты играешь в онлайн-игры,** то используй псевдоним, то есть выдуманное, а не настоящее имя.
- 15 Обсуждай с родителями, в какие игры ты играешь и что смотришь в Интернете.** В играх и видео в Интернете иногда показывают плохое поведение или говорят плохие слова. Выбирай вместе с родителями только безопасные сайты, игры и видео. Всегда спрашивай взрослых, если что-то непонятно.
- 16 Не всему в Интернете можно доверять.** Проверяй вместе с родителями или учителями информацию и источники, особенно новости и заманчивые предложения. Избегай подозрительных ссылок и сообщений, чтобы не скачать вирусы или не попасть на обман.
- 17 Совершай покупки в Интернете только вместе с родителями.** Не покупай ничего в личных сообщениях в социальных сетях или мессенджерах — так мошенники могут украсть деньги или доступ к твоим аккаунтам.
- 18 Никогда не сообщай никому кроме родителей ПИН-код банковской карты и коды из СМС-уведомлений.**
- 19 Участвуй только в тех онлайн-занятиях, которые разрешают и предлагают родители и учителя.** Это могут быть олимпиады, конкурсы, курсы или вебинары.



Эти правила помогут тебе защитить себя от различных неприятностей в Интернете, а также создать безопасное и позитивное пространство для себя и других.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

Если что-то тебя настораживает или пугает – обязательно обратись к родителям или учителям за поддержкой и помощью!

Телефоны доверия, горячие линии

- ✳ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации** (бесплатно, круглосуточно) **8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации.
- ✳ **Всероссийский Детский телефон доверия** (бесплатно, круглосуточно) **8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям.
- ✳ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации** (бесплатно, круглосуточно) **8-800-100-12-60#1**
- ✳ **Горячая линия поддержки по вопросам травли Травли.NET** **8-800-500-44-14** (ПН-ПТ с 10:00 до 20:00 по московскому времени).

2. РЕКОМЕНДАЦИИ ДЛЯ ПОДРОСТКОВ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Привет, дорогой друг!

Современный мир стремительно меняется, развиваются онлайн-технологии, различные гаджеты и девайсы, которые все мы используем в повседневной жизни. Интернет также стал некоторой частью нашей реальности и инструментом, с помощью которого можно общаться, учиться, узнавать новое. И, как с любым инструментом, им нужно пользоваться аккуратно, помня о некоторых рисках и угрозах виртуального мира.

Если ты во время учебы или досуга используешь Интернет и его ресурсы на смартфоне, планшете или персональном компьютере, пожалуйста, воспользуйся следующими рекомендациями. Они помогут тебе быть более компетентным, осознанным, внимательным и осмотрительным в онлайн-пространстве, проявить заботу о себе, своих близких и других людях.

1 Помни о защите своей личной информации

Не делись в онлайн своими или чужими личными данными: никогда не публикуй свои фамилию и имя, полную дату рождения, домашний адрес, номер телефона, номер школы и класса, в которых учишься, информацию о семье или другую личную информацию в Интернете. Этими сведениями могут воспользоваться злоумышленники. Даже твои фото, видео и голосовые сообщения могут быть ими использованы. Используй никнеймы (псевдонимы) при регистрации на сайтах, в социальных сетях, мессенджерах или в играх, а не свое настоящее имя.



ИСКЛЮЧЕНИЕ: официальные платформы (например, Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг» или Госуслуги) и мессенджеры (например, Сферум, Max).

2 Используй настройки конфиденциальности

На мобильных устройствах, в мессенджерах, социальных сетях, чтобы ограничить доступ к твоей информации. Убедись, что твои профили и аккаунты настроены так, чтобы только близкие, друзья и учителя могли видеть личную информацию. Если ты активно ведешь свою страницу, канал или паблик, ограничь доступ к своим постам: настрой видимость своих публикаций так, чтобы их могли видеть только те, кому ты доверяешь (родители, близкие родственники, друзья, возможно учителя).



3 Применяй безопасные пароли и не сообщай их никому

Надежный пароль — это сложный пароль, состоящий из заглавных и строчных букв, цифр и символов. Обычно его трудно угадать или подобрать. Не используй один и тот же пароль для разных аккаунтов. Никогда не делись своими паролями с другими, даже с друзьями. Регулярно меняй пароли, чтобы обезопасить себя.



4 Используй антивирусное программное обеспечение и файрвол (межсетевой экран, брандмауэр)

Для защиты от вредоносных программ и нежелательного трафика используй антивирусы и системы безопасности, которые действуют как барьер между компьютерной сетью и внешним миром.



5 Обсуждай вопросы онлайн-безопасности с родителями или учителями

Сообщай о проблемах: если кто-то угрожает тебе или ты чувствуешь себя некомфортно в Интернете, расскажи об этом родителям или учителям. Обращаться за помощью и принимать ее — важный навык современного человека.

Сохраняй доказательства: если ты стал жертвой кибертравли (кибербуллинга), другого онлайн-насилия или мошенничества, сохраняй скриншоты и сообщения как доказательства. Помни о кибербуллинге: если ты стал жертвой онлайн-травли, сообщи об этом взрослым.

Будь внимателен к онлайн-играм или медиаконтенту: некоторые игры могут содержать агрессивное поведение, а видео и фото — неподобающий, токсичный контент. Обсуждай с родителями, в какие игры ты играешь, какие онлайн-платформы и контент тебе интересны.



6 Старайся придерживаться безопасного общения

Интернет так устроен, что иногда может сложиться иллюзия доверия, безопасности, анонимности и конфиденциальности. Может показаться, что ты хорошо знаешь человека, с которым в реальной жизни никогда не встречался, но уже какое-то время общаешься онлайн. Но это может быть небезопасным. Поэтому не общайся с незнакомыми людьми в Интернете и не принимай запросы в друзья от тех, кого не знаешь в реальной жизни. Не отправляй личные сообщения незнакомцам: будь осторожен с тем, что ты пишешь и отправляешь в личных сообщениях. Не встречайся с людьми из Интернета, это могут быть злоумышленники.

Если кто-то в Интернете ведет себя странно или пытается заставить тебя делать что-то, что вызывает у тебя стыд, или спрашивает тебя о том, о чем ты не хочешь говорить, задает много вопросов о твоей семье, прекрати общение и сообщи об этом взрослым. Самый надежный способ позаботиться о себе — прервать контакт с незнакомым пользователем, который может писать или звонить тебе.



7 Позаботься о своей кибергигиене

Старайся ограничить время, проведенное в Интернете. Делай перерывы и занимайся другими видами деятельности, чтобы избежать переутомления, усталости глаз и зависимости от цифровых устройств.

8 Участвуй только в безопасных онлайн-активностях

Выбирай безопасные сайты и приложения, используй только проверенные платформы для общения и игр. Участвуй в тех образовательных онлайн-активностях (олимпиадах, конкурсах, курсах, вебинарах и других событиях), которые проверены твоими близкими взрослыми, и которые помогут тебе развивать навыки и знания.



9 Развивай критическое мышление

Проверяй и перепроверяй информацию: не верь всему, что видишь в интернете. Проверяй факты и источники информации, особенно если это касается новостей или заманчивых предложений.

Будь осторожен с рекламой: не кликай на подозрительные ссылки, которые могут привести к вирусам или мошенничеству. Помни, что ссылки из подозрительных писем, сообщений и постов в мессенджерах или социальных сетях могут содержать вредоносное программное обеспечение и заразить твой компьютер или мобильное устройство.

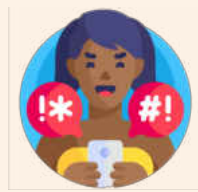


10 Будь бдителен при онлайн-покупках

Не доверяй сайтам, которые выглядят подозрительно, и проверяй отзывы о продавцах перед покупкой товаров онлайн. Совершай покупки только вместе с родителями.

Не делай покупки в личных сообщениях в мессенджерах или социальных сетях: мошенники могут получить доступ и контроль к денежным средствам и твоим аккаунтам.

Будь предельно осторожен с предложениями сделать донат (добровольное денежное пожертвование).



11 Никогда не продавай свои аккаунты в мессенджерах, социальных сетях, онлайн-играх, а также СИМ-карты и банковские карты!

Мошенники могут воспользоваться ими в корыстных целях, но ответственность придется нести тебе, твоим родителям и близким. Никогда не сообщай номер, ПИН-код, CVC-код и другие данные своей банковской карты, а также коды из СМС-уведомлений и электронных писем посторонним людям.



12 Изучи правила и нормы поведения в Интернете

Придерживайся правил, чтобы избежать конфликтов и неприятных ситуаций. Соблюдай законы, действующие в нашей стране — они также распространяются на поисковые запросы, поведение людей в Интернете и публикуемый ими контент.

Будь осторожен с публикациями в социальных сетях и сообщениями в мессенджерах. То, что кажется забавным или безобидным, может нарушать закон, или оказаться вирусным и быстро распространиться среди большой, не всегда желательной, аудитории. Прежде чем разместить пост или отправить сообщение, внимательно оценивай его содержание. **Помни:** Интернет — это публичное пространство, и необдуманные поступки могут иметь серьезные последствия.

Если ты столкнулся с противоправным контентом в Интернете, сообщи об этом родителям и/или учителям, а также отправь ссылки и скриншоты в правоохранительные органы и Роскомнадзор.



Кибербезопасность, цифровая грамотность, навыки распознавания онлайн-рисков — это важный аспект твоей жизни в современном мире!

Следуя этим рекомендациям, ты сможешь защитить себя от различных онлайн-угроз, а также создать безопасное и позитивное онлайн-пространство для себя и других.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ

Телефоны доверия, горячие линии

- ✳ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- ✳ **Всероссийский Детский телефон доверия 8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- ✳ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
 - Также для обращения доступна короткая комбинация **123** (бесплатно, круглосуточно).
- ✳ **Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
 - ПН-ПТ с 10:00 до 20:00 по московскому времени.

Онлайн-помощь

- Горячая линия «Дети Онлайн» <http://detionline.com/helpline/about>
- ЧАТ-БОТ «Добрыня» (антибуллинг) <https://t.me/BylingBot>
- Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь» — сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете <https://youthombudsman.ru/help>
- Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

Информационно-методические материалы и ресурсы

- Касперский детям <https://kids.kaspersky.ru/>

3. РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) ПО КИБЕРБЕЗОПАСНОСТИ ДЕТЕЙ И ПОДРОСТКОВ

Уважаемые родители!

В современном мире, насыщенном цифровыми технологиями, вопрос кибербезопасности становится все более актуальным. Дети и подростки активно используют Интернет для общения, учебы и развлечений, и важно, чтобы они понимали риски и умели защищать себя в виртуальном пространстве.

Проблема кибербезопасности заключается в том, что Интернет может быть источником не только полезной информации, но и угроз. Дети и подростки могут столкнуться в онлайн с мошенничеством, кибербуллингом, вредоносным контентом и другими опасностями. Это может привести к негативным последствиям для их психического здоровья, репутации и даже физической безопасности.

Нам, взрослым, необходимо уделять внимание вопросам кибербезопасности наших детей. Обсуждая с ними правила безопасного поведения и использования онлайн-пространства, объясняя, как распознавать те или иные риски, мы можем научить детей быть устойчивыми и защищенными в сети Интернет.

ВАЖНО

Медицинские и психолого-педагогические исследования, а также рекомендации СанПиН показывают, что использование электронных устройств и Интернета лучше **полностью исключить в раннем детстве (до 3 лет)**. Намного полезнее для детей живое общение, продуктивная развивающая деятельность, чтение, рисование и игры со сверстниками.

В старшем дошкольном возрасте экранное время может составлять **не более 1 часа в день** и только в присутствии взрослых. **В младшем школьном возрасте** продолжительность использования цифровых устройств **не должна превышать 1,5 часов**. **В подростковом и юношеском возрастах — не более 2 часов в день**.

При этом во всех возрастах непрерывный просмотр или онлайн-активность должны чередоваться с гимнастикой для глаз и другими видами интеллектуальной и физической деятельности. Каждый родитель, опираясь на рекомендации, стоит перед серьезным решением: определить, сколько времени пойдет его ребенку на пользу с учетом возраста, учебы, общения и отдыха.

Вы можете воспользоваться следующими простыми рекомендациями, чтобы помочь детям и подросткам быть более компетентными, осознанными, внимательными и осмотрительными в интернет-среде.



1 Обучайте детей и подростков основам кибербезопасности

- ✦ Поговорите с детьми о том, почему важно защищать личные данные и как это может помочь избежать проблем.
- ✦ Проверяйте настройки конфиденциальности и научите детей создавать надежные пароли, использовать двухфакторную аутентификацию и не делиться с незнакомцами личной информацией в Интернете.
 - **Надежный пароль** — это сложный пароль, состоящий из букв, цифр и символов. Обычно его трудно угадать или подобрать. Важно периодически менять пароли в мессенджерах, электронной почте и социальных сетях.
 - **Личная информация** — фамилия и имя, полная дата рождения, домашний адрес, номер телефона, номер школы и класса, информация о семье, другая личная информация (например, паспортные данные, данные медицинского полиса, СНИЛС и др.). Этими сведениями могут воспользоваться злоумышленники. Даже фото, видео и голосовые сообщения могут быть ими использованы.
- ✦ Используйте надежное антивирусное программное обеспечение на Ваших устройствах и регулярно обновляйте его. Обсуждайте с ребенком или подростком важность защиты от вредоносных программ.
- ✦ Рассказывайте о подозрительных людях в Интернете. Объясните ребенку или подростку, что не стоит общаться с незнакомцами в сети Интернет, и что делать, если кто-то ведет себя странно или пытается заставить делать что-то неприемлемое.
- ✦ Помогите детям и подросткам понять и осознать, почему не стоит отвечать на сообщения и звонки с незнакомых номеров по мобильной связи, в мессенджерах и социальных сетях. Объясните, что это может привести к нежелательным контактам и опасности.
- ✦ Обучайте распознаванию подозрительных ссылок. Расскажите ребенку или подростку о рисках перехода по ссылкам из неизвестных источников и научите его проверять ссылки перед переходом.

2 Обсуждайте и устанавливайте семейные правила использования Интернета и кибергигиены

- ✦ Определите вместе с ребенком или подростком, сколько времени он может проводить в Интернете, какие сайты он может посещать и с кем общаться, какие мессенджеры и социальные сети он может использовать.
- ✦ Если Ваш ребенок старшего дошкольного или младшего школьного возраста пользуется мобильным устройством или персональным компьютером, установите программы родительского контроля, чтобы ограничить доступ к нежелательному контенту и отслеживать активность в Интернете.
- ✦ Установите разумные ограничения на использование цифровых устройств и перерывы для других видов деятельности. Это поможет избежать переутомления и зависимости от Интернета.

3 Поддерживайте атмосферу доверия и регулярно обсуждайте с ребенком или подростком онлайн-опыт

- ✦ Поощряйте детей и подростков обсуждать с Вами вопросы, связанные с Интернетом и информационной безопасностью, делиться своими переживаниями, опасениями и проблемами, связанными с онлайн-пространством, без страха наказания. Проводите беседы о том, что делают дети в Интернете, с кем общаются, во что играют, какие сайты посещают, какой медиаконтент им интересен, и обсуждайте возможные риски. Рассмотрите возможность совместного просмотра контента и обсуждения увиденного.

4 Будьте примером для подражания

- ✦ Показывайте ребенку или подростку, как Вы сами соблюдаете правила информационной безопасности, и обсуждайте с ним Ваши совместные действия в Интернете. Показывайте, как правильно вести себя в Интернете, не нарушайте правила и нормы поведения в онлайн при ребенке, объясняйте, почему важно соблюдать эти правила.

5 Развивайте у детей навыки обращения за помощью и сообщения об опасности Вам и другим надежным взрослым (родственникам, учителям, сотрудникам правоохранительных органов)

- Обучайте детей и подростков тому, как фиксировать онлайн-риски с помощью скриншотов, сохранения видео- и аудиосообщений от незнакомцев. Все это может стать серьезной доказательной базой в критических ситуациях. Этот навык может помочь не только в виртуальном мире, но и в реальной жизни.

6 Помогайте детям и подросткам развивать критическое мышление

- Научите их анализировать информацию в Интернете, распознавать опасности: объясните, как распознавать мошенничество, кибертравлю и другие формы онлайн-угроз. Приводите примеры кибервиктимизации, ненадлежащего, рискованного и опасного онлайн-поведения, чтобы дети и подростки могли лучше понять, как избежать подобных ситуаций.
- Развивайте у ребенка аналитические навыки, чтобы он мог оценивать информацию в Интернете, сомневаться в достоверности источников и отличать достоверные источники от недостоверных. Расскажите, что не вся информация в Сети является правдивой.
 - Придумайте «волшебное слово-пароль», которое будете знать только Вы и Ваш ребенок, чтобы он мог распознать опасность: в случае, если ребенок ответил на сообщение или звонок незнакомца, с помощью этого слова ему будет проще распознать опасность.

7 Проявляйте поддержку и вовлеченность

- Постарайтесь быть вовлеченными в онлайн-активности: участвуйте в играх и социальных сетях вместе с детьми и подростками, чтобы лучше понять их интересы и окружение, это позволит поддерживать доверительный контакт с ними.
- Поощряйте детей и подростков заниматься безопасными и конструктивными офлайн и при необходимости онлайн-активностями, такими как образовательные игры, спорт или творческие проекты. Активная, интересная и насыщенная положительными эмоциями и событиями реальная жизнь — мощный источник позитивной самореализации без «бегства» в виртуальный мир.

8 Отработайте совместно с ребенком действия в ситуациях риска

- Важно заранее объяснить ребенку, как правильно действовать при столкновении с опасными онлайн-коммуникациями:
 - не вступать в перепалку, сразу заблокировать агрессора или мошенника, сохранить скриншоты переписки в качестве доказательств и обязательно рассказать о ситуации взрослым — родителям, учителю или обратиться в поддержку платформы, где произошел инцидент.
- Обращайтесь за помощью: если Вы заметили, что Ваш ребенок стал жертвой кибервиктимизации или проявляет опасное поведение в Интернете, не стесняйтесь обращаться за помощью к специалистам.

9 Регулярно обновляйте знания о кибербезопасности и кибергигиене, отслеживайте изменения в законодательстве и правилах платформ

- Следите за новостями и тенденциями в области кибербезопасности, изучайте новые методы защиты от киберпреступлений. Будьте в курсе изменений в законодательстве и правилах использования платформ, чтобы обеспечить максимальную защиту Вашего ребенка или подростка, адаптируйте свои подходы к обеспечению безопасности в соответствии с изменениями в Интернете.

Алгоритм действий родителя при обнаружении подозрительной онлайн-активности ребенка

- Обратите внимание на изменения в поведении ребенка или подростка. Если Вы заметили, что он стал более замкнутым, погруженным в онлайн, раздражительным или проявляет другие нетипичные для него эмоции, это может быть сигналом о проблемах в Интернете.
- Поговорите с ребенком. Выясните, что именно его беспокоит, и предложите свою помощь.
- Обратитесь за помощью к специалистам. Если Вы не можете самостоятельно решить проблему, обратитесь к психологу, социальному педагогу, психотерапевту или другим специалистам.

В ситуациях, когда ребенок сообщает Вам о совершенном в отношении него преступлении воспользуйтесь 8 памяткой [Навигатора профилактики виктимизации детей и подростков \(2024\)](#)



Более подробные рекомендации для родителей Вы найдете в пособии [«Риски в цифровой среде: диагностика, профилактика, коррекция»](#). — М: АНО «Центр глобальной ИТ-кооперации», 2024. — 152 с.



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ



Телефоны доверия, горячие линии

- Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- Всероссийский Детский телефон доверия 8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
 - Также для обращения доступна короткая комбинация **123** (бесплатно, круглосуточно).
- Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
 - ПН-ПТ с 10:00 до 20:00 по московскому времени.

Онлайн-помощь

- Горячая линия «Дети Онлайн» <http://detionline.com/helpline/about>
- ЧАТ-БОТ «Добрыня» (антибуллинг) <https://t.me/BylingBot>
- Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь» — сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете <https://youthombudsman.ru/help>
- Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

Информационно-методические материалы и ресурсы

- Касперский детям <https://kids.kaspersky.ru/>

4. РЕКОМЕНДАЦИИ ДЛЯ СПЕЦИАЛИСТОВ ПО РАЗВИТИЮ МЕДИАКОМПЕТЕНЦИЙ У ДЕТЕЙ И ПОДРОСТКОВ

Уважаемые коллеги!

В современном мире цифровые технологии стали неотъемлемой частью нашей жизни. Но, как и любые инструменты, Интернет и различные устройства не только позволяют нам и нашим детям обретать новые знания, расширять возможности общения или проведения досуга, но и несут в себе различные онлайн-риски и угрозы. Поэтому важно, чтобы дети и подростки умели правильно и безопасно взаимодействовать с онлайн-средой.

Вы можете использовать данную памятку как основу для разработки профилактических, развивающих, психокоррекционных и просветительских программ, направленных на повышение осведомленности детей и подростков о рисках в Интернете, формирование навыков безопасного поведения в киберпространстве и развитие их медиакомпетенций.

Отметим, что **профилактика** в первую очередь направлена на **развитие** с учетом возрастных особенностей детей и подростков **личностных ресурсов**, способствующих преодолению различных трудных жизненных ситуаций и влияющих на **повышение устойчивости** к неблагоприятным факторам.

Поэтому с детьми и подростками целесообразно проводить занятия, которые в целом развивают такие ресурсы как:

- ✳ когнитивные способности, интерес к учебе и духовному росту, чувство юмора,
- ✳ просоциальные увлечения и широкий круг интересов,
- ✳ эмоциональный интеллект и эмоциональная зрелость,
- ✳ внутренний самоконтроль, целеустремленность, успешное овладение навыками принятия решений,
- ✳ ответственное поведение и правосознание, уважение законов и норм общества, школы, семейных стандартов,
- ✳ умение обращаться за помощью,
- ✳ возможность активного участия в работе социальной группы,
- ✳ доверительные отношения с родителями (законными представителями),
- ✳ общение среди просоциальных сверстников и другие.



Помимо этого в процессе профилактики онлайн-рисков, опасного поведения детей и подростков в Интернете и в ходе развития медиакомпетенций у детей и подростков можно опираться на следующие рекомендации.

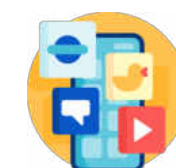
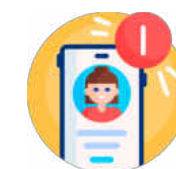
1 Обучение основам кибербезопасности и формирование навыков безопасного общения

- ✳ Информируйте детей и подростков о принципах кибербезопасности: создании надежных паролей, использовании двухфакторной аутентификации, настройках конфиденциальности в социальных сетях и других онлайн-платформах.
- ✳ Познакомьте детей с приложениями и инструментами, которые помогают оставаться в безопасности в Интернете, например, с программами родительского контроля, антивирусами и настройками конфиденциальности.
- ✳ Проводите занятия, на которых можно обсудить правила безопасного общения в Интернете. Важно говорить об уважении к другим пользователям и недопустимости агрессивного поведения.



2 Развитие критического мышления и навыков анализа информации

- ✳ Организуйте занятия, на которых дети и подростки смогут изучить основы критического мышления, включая анализ, оценку и интерпретацию данных.
- ✳ Научите детей различать надежные и ненадежные источники информации, объясняя, какие факторы следует учитывать (авторитет, дата публикации, цель и т.д.).
- ✳ Сформируйте навыки использования ресурсов и поисковых систем для поиска информации, проверки ее достоверности и фактов, приводите примеры фейковых новостей и дезинформации, чтобы помочь детям и подросткам понять, как они могут выглядеть и какие последствия они могут иметь.
- ✳ Обсуждайте онлайн-контент: проводите занятия, на которых подростки смогут анализировать и обсуждать информацию из Интернета, включая новости, рекламу и социальные сети.
- ✳ Развивайте навыки распознавания фейковых новостей: научите детей различать достоверные источники информации и фейковые новости, обсуждая примеры и методы проверки фактов.
- ✳ Проводите дискуссии о социальных сетях: обсуждайте, как информация распространяется в социальных сетях, и как это может влиять на восприятие реальности.



3 Развитие навыков задавания вопросов

- ✳ Научите детей задавать вопросы о том, что они читают или видят в Интернете. Например, «Кто это написал?», «Каковы его источники?» и «Почему это важно?».
- ✳ Разработайте вместе с детьми список вопросов, которые они могут задавать при оценке информации.



4 Осведомленность о рисках онлайн и офлайн

- ✳ Информировать о кибертравле и кибервиктимизации: обсуждайте с детьми и подростками, что такое кибербуллинг, как его распознать и как действовать в случае его возникновения.
- ✳ Обсуждайте реальные случаи: приводите с учетом возраста детей и подростков примеры кибервиктимизации и мошенничества, чтобы помочь им понять, как избежать подобных ситуаций.



5 Обучение распознаванию манипуляций в онлайн и офлайн

- ✳ Обсуждайте методы манипуляций, которые используют злоумышленники и мошенники: объясните, как используются эмоциональные триггеры, манипуляции и пропаганда для влияния на мнение людей.
- ✳ Анализируйте рекламные материалы: проводите занятия, на которых дети могут анализировать рекламу и пропаганду, чтобы понять, как они могут быть обмануты.



6 Развитие навыков саморегуляции

- ✳ Обучайте управлению временем: помогите детям и подросткам установить разумные лимиты на время, проведенное в Интернете, и научите их управлять своим временем.
- ✳ Поощряйте активный отдых: напоминайте детям и подросткам о важности физической активности и хобби вне Интернета, чтобы сбалансировать их активность в онлайн и офлайн.



7 Создание безопасной атмосферы для обсуждений и поддержка открытого общения

- ✳ Создайте атмосферу, в которой дети и подростки могут делиться своими переживаниями и проблемами, мыслями и сомнениями, связанными с Интернетом, без страха осуждения.
- ✳ Проводите регулярные беседы о том, что они делают в Интернете, с кем общаются, и какие у них есть вопросы или опасения, а также о том, что они читают и видят в онлайн-пространстве, и обсуждайте, как это может быть связано с реальностью.



8 Сотрудничество с родителями (законными представителями)

- ✳ Проводите семинары для родителей (законных представителей), чтобы они могли лучше понимать онлайн-риски и поддерживать своих детей в безопасном поведении в Интернете, в развитии у них критического мышления и распознавании недостоверной информации.



9 Использование интерактивных методов

- ✳ Включайте игры, дискуссии, групповые занятия и проекты, чтобы сделать обучение более увлекательным и запоминающимся.
- ✳ Используйте ролевые игры для отработки ситуаций, связанных с общением в Интернете, чтобы помочь детям научиться реагировать на потенциальные угрозы.



Подробные рекомендации по просвещению Вы найдете в пособии **«Организация просветительской работы с родителями по вопросам профилактики девиантного поведения»**. – Москва : ФГБОУ ВО МГППУ, 2018. – 112 с.



КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ И ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ

Телефоны доверия, горячие линии

- ✳ **Горячая линия кризисной психологической помощи Министерства просвещения Российской Федерации 8-800-600-31-14**
 - На линии ежедневно и круглосуточно оказывается психологическая помощь и поддержка всем позвонившим, находящимся в кризисном состоянии или в кризисной ситуации (бесплатно, круглосуточно).
- ✳ **Всероссийский Детский телефон доверия 8-800-2000-122**
 - Психологическое консультирование, экстренная и кризисная психологическая помощь детям, подросткам и родителям (бесплатно, круглосуточно).
- ✳ **Горячая линия «Ребенок в опасности» Следственного комитета Российской Федерации 8-800-100-12-60#1**
 - Также для обращения доступна короткая комбинация 123 (бесплатно, круглосуточно).
- ✳ **Горячая линия поддержки по вопросам травли Травли.NET 8-800-500-44-14**
 - ПН-ПТ с 10:00 до 20:00 по московскому времени.

Онлайн-помощь

1. Горячая линия «Дети Онлайн»
<http://detionline.com/helpline/about>
2. Раздел «Кибербуллинг» портала Минцифры и Ростелекома <https://xn----9sbbihqekoax4a5b.xn--p1ai/>
3. Сайт Молодежного цифрового омбудсмена, раздел «Цифропомощь»: сервис подачи обращений для молодых людей, которые столкнулись с проблемами в Интернете
<https://youthombudsman.ru/help>
4. Сообщить о запрещенном контенте можно на сайте Роскомнадзора <https://eais.rkn.gov.ru/feedback/>

Информационно-методические материалы и ресурсы

1. Образовательный портал Альянса по защите детей в цифровой среде «ЦИФРАтека. База практических знаний»
<https://cifrateka.ru/>
2. Вестник Киберполиции России
<https://max.ru/cyberpolice>
3. Касперский детям <https://kids.kaspersky.ru/>
4. Материалы АНО «Центр изучения и сетевого мониторинга молодежной среды»
<https://www.cism-ms.ru/poleznye-materialy/>

Куда можно направить родителей (законных представителей)

1. Портал Растимдетей.рф — навигатор для современных родителей по вопросам развития, воспитания и образования детей от 0 до 18 лет (статьи, памятки, буклеты).
2. Психологический университет для родителей «Быть родителем» — bytyroditel.ru