0.5. НОРМАТИВНО-ПРАВОВАЯ БАЗА В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОФИЛАКТИКИ СОЦИАЛЬНЫХ РИСКОВ В СЕТИ ИНТЕРНЕТ

Информационная безопасность

- Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Федеральный закон Российской Федерации от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646 от 5 декабря 2016 года).
- Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утверждена Указом Президента Российской Федерации от 9 мая 2017 года № 203).
- Концепция информационной безопасности детей в Российской Федерации (утверждена распоряжением Правительства Российской Федерации от 28 апреля 2023 года № 1105-р).

Профилактика негативных социальных явлений в детской и молодежной среде, правонарушений среди несовершеннолетних, межведомственное взаимодействие

- Федеральный закон Российской Федерации от 24 июля 1998 года № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».
- Федеральный закон Российской Федерации от 24 июня 1999 года № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних».
- Федеральный закон Российской Федерации от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации».
- Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024–2028 годы (утвержден Указом Президентом Российской Федерации 30 декабря 2023 года № Пр-2610).
- Стратегия противодействия экстремизму в Российской Федерации (утверждена Указом Президента Российской Федерации от 28 декабря 2024 года № 1124).
- Концепция развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 22 марта 2017 года № 520-р).
- План основных мероприятий, проводимых в рамках Десятилетия детства, на период до 2027 года (утвержден распоряжением Правительства Российской Федерации от 23 января 2021 года № 122-р).
- Стратегия комплексной безопасности детей в Российской Федерации до 2030 года (утверждена Указом Президента Российской Федерации от 17 мая 2023 года № 358).
- План мероприятий по реализации Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года (утвержден распоряжением Правительства Российской Федерации от 17 ноября 2023 года № 3233-р).
- Комплекс мер по профилактике негативных социальных явлений в детской и молодежной среде на 2023–2025 годы (утвержден распоряжением Правительства Российской Федерации от 24 июня 2023 года № 1667-р).
- Концепция развития системы психолого-педагогической помощи в сфере общего образования и среднего профессионального образования в Российской Федерации на период до 2030 года (утверждена приказом Минпросвещения России 18 июня 2024 года № СК-13/07вн).

НОРМАТИВНО-ПРАВОВАЯ БАЗА В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОФИЛАКТИКИ СОЦИАЛЬНЫХ РИСКОВ В СЕТИ ИНТЕРНЕТ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОФИЛАКТИКЕ РИСКОВ В СЕТИ ИНТЕРНЕТ

- **Комплект памяток для педагогических работников и иных профильных специалистов по их действиям в ситуациях социальных рисков и профилактике девиантного поведения обучающихся «Навигатор профилактики»** с учетом разработанных критериев выявления изменений в поведении детей, которые могут свидетельствовать о рисках совершения общественно опасного деяния, киберагрессии, интернет-зависимости (письма Минпросвещения России от 13 декабря 2022 года № 07-8351, от 27 декабря 2022 года № 07-8747, от 26 ноября 2024 года № 07-5707).

- **Памятки для родителей и несовершеннолетних по информационной безопасности** (письмо Минпросвещения России от 24 мая 2023 года № 07–2755).

- **Рекомендации по использованию медиативных технологий в социальных сетях** (письмо Минпросвещения России от 14 августа 2024 года № ДГ-1333).

- **Методические рекомендации для педагогических работников дошкольных образовательных организаций по формированию у воспитанников основ безопасного поведения** (на природе, на дорогах, на объектах транспортной инфраструктуры, на транспорте, в быту, социуме, информационном и цифровом пространстве (письмо Минпросвещения России от 18 июня 2024 года № 03-881, размещены на официальном сайте ФГБНУ «Институт развития, здоровья и адаптации ребенка»).

- **Методические рекомендации по обеспечению психологической безопасности образовательной среды, в том числе профилактике травли, интернет-травли** (письмо Минпросвещения России от 24 мая 2023 года № 07–2755).

Навигатор профилактики девиантного поведения (2022)

Навигатор профилактики виктимизации детей и подростков (2024)

1. СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКАЯ ДЕЗАДАПТАЦИЯ И ПСИХОЭМОЦИОНАЛЬНОЕ НАПРЯЖЕНИЕ У ДЕТЕЙ И ПОДРОСТКОВ

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКАЯ ДЕЗАДАПТАЦИЯ – это состояние, осложняющее приспособление к социальной среде и окружению. Проявляется в первую очередь в офлайн реальности и не является видом девиантного (отклоняющегося) поведения.

Часто дети и подростки, пережившие или находящиеся в кризисных и/или объективно/субъективно трудных жизненных ситуациях, могут демонстрировать это состояние. Также дезадаптация может предшествовать проявлениям различных видов отклоняющегося поведения, в том числе в онлайн-пространстве, или быть его следствием.

Проявления дезадаптации могут варьироваться от незначительных трудностей в общении до серьезных поведенческих или психических расстройств, без оказания соответствующей комплексной помощи приобретающих хронический характер.

С чем может быть связана социально-психологическая дезадаптация?

Ситуации, связанные с легко прогнозируемыми жизненными обстоятельствами:

- Поступление в школу, переход из класса в класс или на другую ступень обучения (включая этап подготовки к выпуску из образовательной организации).
- Смена классного руководителя.
- Экзаменационные ситуации.
- Нововведения в учебном процессе и другие ситуации.

Различные сочетания нижеуказанных общих признаков могут свидетельствовать о социально-психологической дезадаптации:

- Резкое снижение успеваемости, в том числе связанное с нарушением учебной мотивации.
- Отказ посещать школу.
- Проблемы в межличностных отношениях.
- Нетипичные для ребенка эмоциональные реакции.
- Физиологические реакции, например слабость, жалобы на головные боли и/или боли в животе, дрожь и другие проявления.
- Навязчивые движения и действия (накручивает волосы на палец или выдергивает, грызет ногти, а также разговаривает сам с собой, и другие проявления).
- Конфликтное, агрессивное отношение к окружающим, в том числе в сети Интернет.

Ситуации, связанные с непредвиденными жизненными обстоятельствами и различными социальными рисками:

- Внезапная смена образовательной организации.
- Проблемы взаимоотношений и конфликты.
- Трудные, опасные или кризисные ситуации, жестокое обращение и различные виды насилия, пренебрежение нуждами ребенка и преступления, совершаемые в окружении или в отношении обучающегося.
- Переживание горя (развод родителей, болезнь, расставание или смерть кого-то из близких или друзей, а также домашних животных, собственные заболевания).
- Потеря родителями работы.
- Чрезвычайные и экстремальные ситуации, которые наблюдает или о которых случайно узнает обучающийся, и другие ситуации.

Социально-психологическая дезадаптация может проявляться у детей и подростков в стрессовых реакциях, тревожности, депрессии, замкнутости, низкой самооценке, социальном отвержении, проблемах в обучении и коммуникации, трудностях в построении доверительных отношений, агрессивных реакциях и социальной интеграции.

Риски, связанные с социально-психологической дезадаптацией:

- Психосоматические расстройства/заболевания (ребенок начинает часто болеть и просто не ходить в школу, получая вполне надежные медицинские справки).
- Различные виды девиантного (отклоняющегося) поведения, в том числе в сети Интернет.

ВАЖНО своевременное вмешательство, включающее профессиональную помощь специалистов (психологов, социальных педагогов, врачей, социальных работников и др.), а также поддержку семьи и окружающего сообщества, чтобы способствовать адаптации ребенка или подростка.

Во время взаимодействия с ребенком **важно обращать внимание** на проявления **психоэмоционального и/или нервно-психического напряжения**, которые могут дополнительно указывать на признаки социально-психологической дезадаптации.

ПСИХОЭМОЦИОНАЛЬНОЕ НАПРЯЖЕНИЕ — это состояние организма, характеризующееся повышенным уровнем стресса, тревоги и эмоциональной нестабильности. Оно может:

- возникать в ответ на различные стрессовые факторы, психоэмоциональные нагрузки, кризисные и опасные ситуации,
- проявляться через такие симптомы, как раздражительность, усталость, снижение концентрации внимания и работоспособности, нарушение сна, а также физические симптомы, такие как учащенное сердцебиение, потливость или мышечное напряжение.

Длительное психоэмоциональное напряжение может негативно влиять на физическое и психическое здоровье ребенка, поэтому важно своевременно предпринимать меры для его снижения и поиска способов управления стрессом.

Почему дети и подростки с признаками социально-психологической дезадаптации переносят социальную активность в Интернет?

- **Избегание реальности** — возможность уйти от проблем и стрессов, связанных с реальной жизнью, таких как буллинг, трудности в учебе или проблемы в семье.
- **Поиск поддержки среди сверстников**, которые испытывают похожие проблемы, что помогает чувствовать себя менее одинокими и более понятыми.
- **Иллюзия анонимности,** снижающая страх перед осуждением и позволяющая свободно выражать свои мысли и чувства.
- **Поиск информации о проблемах,** с которыми они сталкиваются, чтобы лучше понять себя и свои чувства.
- **Развлечение и отвлечение:** игры, видео и другие формы контента помогают отвлечься от негативных эмоций и расслабиться.
- **Виртуальное общение** может быть более комфортным для тех, кто испытывает трудности в реальных социальных взаимодействиях.

Во время взаимодействия с ребенком или подростком рекомендуется:

01 Учитывать динамику и протяженность проявления признаков социально-психологической дезадаптации.

02 Обсудить на психолого-педагогическом консилиуме (ППк) с другими учителями, ведущими разные предметы в этом классе, и специалистами школы возможные варианты индивидуальной помощи ребенку с целью преодоления учебных трудностей, либо необходимость разработки индивидуального учебного плана до уровня полного восприятия материала, пока ребенок не почувствует успех.

03 Дать почувствовать ребенку, что его состояние, отличающееся от обычного, замечено, и учитель открыт к тому, чтобы оказать поддержку, если ребенок в ней нуждается:

- Мне кажется, что тебя что-то беспокоит или у тебя что-то происходит. Если тебе нужно поговорить, я всегда готов(а) тебя выслушать.
- Я очень беспокоюсь о том, что с тобой что-то происходит. Мы могли бы поговорить и подумать над решением ситуации.
- Возможно, тебе самому(ой) сейчас нелегко, давай вместе подумаем, что с этим можно сделать.
- Мне показалось, что в последнее время ты выглядишь расстроенным(ой), у тебя что-то случилось?

04 Способствовать формированию у ребенка устойчивого позитивного представления о себе, уверенности в себе, волевых качеств через поиск таких видов деятельности, где ребенок мог бы почувствовать ситуацию успеха. Это может быть включение ребенка в коллективно-творческую деятельность, школьное самоуправление, кружки дополнительного образования.

05 Организовать общеклассные мероприятия с использованием интерактивных форм работы для сплочения класса и создания благоприятного психологического климата.

06 Организовать взаимодействие с педагогом-психологом и социальным педагогом для коррекции воздействия негативных факторов, повлекших социально-психологическую дезадаптацию.

07 Привлечь внимание родителей (законных представителей) к проблеме ребенка. Помните, что ребенок может скрывать школьные события от родителей. Старайтесь наладить доверительные отношения с родителями своих учеников.

КУДА ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ

- **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 для детей в трудной жизненной ситуации, подростков и их родителей, педагогов и специалистов в организациях Вашего муниципального образования/субъекта Российской Федерации.

2. КИБЕРАГРЕССИВНОЕ ПОВЕДЕНИЕ

КИБЕРАГРЕССИВНОЕ ПОВЕДЕНИЕ — это поведение, направленное на причинение вреда посредством электронных устройств одному человеку или группе лиц, и воспринимаемое как оскорбительное, уничижительное, приносящее ущерб или нежелательное.

ПРИЗНАКИ КИБЕРАГРЕССИВНОГО ПОВЕДЕНИЯ

Любое психологическое насилие в Интернете:

- Коллективное игнорирование.
- Жестокие розыгрыши.
- Распространение слухов.
- Угрозы.
- Конфликтное, агрессивное отношение к окружающим.
- Оскорбления других учеников/учителей, третьих лиц.
- Насмешки.

Формы киберагрессивного поведения

Онлайн форма

Смешанная форма

Смешанная форма может проявляться не только онлайн, но и офлайн или наоборот.

ПОДВИДЫ КИБЕРАГРЕССИВНОГО ПОВЕДЕНИЯ СМЕШАННОЙ ФОРМЫ

01 **Кибертравля (кибербуллинг)**
систематическое и целенаправленное негативное воздействие на пользователя в социально-сетевой среде с целью причинения психологической травмы.

02 **Киберпровокация (троллинг)**
намеренно провокационные или оскорбительные комментарии к статьям в Интернете, к постам в блогах и соцсетях, сообщения в личных или групповых чатах с целью высмеять, унизить, оскорбить автора поста или пользователя, спровоцировать его на негативную реакцию, создать конфликт между другими комментаторами или пользователями группового чата.

03 **Киберразжигание (флейминг)**
разжигание речевого конфликта не в монологе, а в полилоге с участием множества коммуникантов, эмоционально реагирующих на такую речевую провокацию. Кроме того, в отличие от троллинга, флейминг предполагает прямую словесную атаку непосредственно на коммуниканта.

04 **Киберзлословие (хейтинг)**
унижение, необоснованная критика человека, выражающаяся в виде большого количества комментариев с оскорблениями иногда со стороны группы хейтеров, целью которых зачастую является подрыв репутации конкретной личности.

05 **Киберпритеснение (киберхарассмент)**
адресованные конкретному человеку обычно настойчивые или повторяющиеся слова и действия, которые вызывают у него раздражение, тревогу и стресс и при этом не имеют разумной цели. Киберхарассмент обычно выражается в повторяющихся оскорбительных сообщениях жертве, от которых она чувствует себя морально уничтоженной, которым она не может ответить по причине страха или невозможности идентифицировать преследователя, а иногда к тому же вынуждена оплачивать полученные сообщения.

06 **Кибервыманивание (аутинг)**
получение персональной и/или конфиденциальной информации и публикация ее в сети Интернет или передача тем, кому она не предназначалась.

07 **Киберклевета (дениграция)**
распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

08 **Киберпреследование (сталкинг)**
сбор, накопление и использование личной информации о жертве в целях шантажа, запугивания путем угрозы расправы и т.д.

09 **Киберигнорирование или социальная изоляция**
заключается в вытеснении, игнорировании жертвы в интернет-сообществах. Жертву против ее воли исключают из общих переписок, сообществ, чатов (в том числе школьных), групп.

10 **Видеопубликация избиений (хеппислепинг)**
создание и размещение на популярных порталах видеороликов с записями осуществленных сцен насилия (чаще всего группой в отношении жертвы). Может также реализовываться в прямом эфире и соотноситься с делинквентным поведением.

ПОДВИДЫ КИБЕРАГРЕССИВНОГО ПОВЕДЕНИЯ ОНЛАЙН ФОРМЫ

01 **Кибер рассылка «хлама» (спамерство, несанкционированная рассылка нерелевантного контента)**
совокупность нежелательных, незапрошенных электронных и бумажных рассылок, которые агрессивно и без ведома хозяев заполняют почтовые ящики организаций и граждан.

02 **Киберсамозванство (имперсонация)**
выдача себя за другого пользователя сети Интернет путем использования его пароля доступа к аккаунту в социальных сетях, в блоге, почте, либо создание аккаунта с данными «жертвы» и осуществление от его имени негативного общения с другими пользователями.

03 **Киберподлог (фрейпинг)**
осуществление рассылки информации путем взлома личной страницы в социальных сетях и изменения сведений о ее хозяине, которая оскорбляет или ставит под угрозу как его самого, так и его друзей. Но чаще основная цель подобных действий — выставить объект в смешном, нелепом виде.

04 **Киберразглашение (доксинг)**
свободное опубликование персональных данных в сети Интернет, таких как адрес места жительства, логины и пароли учетных записей сайта Госуслуг (Единого портала государственных и муниципальных услуг) или личного кабинета налогоплательщика, переписка, интимные фотографии.

05 **Внутриигровой киберванданлизм (гриффинг)**
процесс, в котором одни игроки целенаправленно преследуют других игроков в многопользовательских онлайн-играх с целью разрушения удовольствия других пользователей от игры путем нарушения отдельного функционала, использования брани, блокирования других пользователей и т.д.

06 **Видеоконференционный вандализм (зумбомбинг, зум-рейдерство)**
преднамеренная атака, когда пользователи получают доступ к видеоконференции и, транслируя различный неприемлемый контент, используя нецензурные выражения, срывают мероприятие, оказывая негативное воздействие на всех его участников.

АЛГОРИТМ ДЕЙСТВИЙ

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

Вынесите этот случай на психолого-педагогический консилиум (ППк) с администрацией и другими специалистами (в том числе приглашенных из других организаций — по необходимости).

Обсудите этот случай с педагогом-психологом, социальным педагогом и представителем школьной службы примирения и/или медиации (при наличии).

Учитывая семейную ситуацию ребенка-агрессора, аккуратно сообщите родителям (законным представителям) о сложившейся ситуации, попросите их не применять насильственные наказания. Объясните ситуацию родителям жертвы.

Совместно с другими специалистами образовательной организации разработайте программу психолого-педагогических и педагогических мероприятий, направленных на профилактику и коррекцию агрессивного поведения, помощь жертве, сплочение учебного коллектива, приступите к реализации этой программы.

По возможности, включите агрессора и жертву в созидательную, интересную им коллективную деятельность, где они оба смогут чувствовать свою причастность к коллективу и осознавать полезность собственных действий.

В случае травли на публичных страницах в социальных сетях, обратитесь к их администратору (если им является другой обучающийся), либо вынесите на психолого-педагогический консилиум предложение обратиться в правоохранительные органы с целью блокировки данной страницы (если администрация канала/паблика/группы/сообщества анонимна или не относится к образовательной организации).

Через некоторое время проведите мониторинг ситуации, убедитесь, что динамика агрессивных проявлений идет на спад.

В случае смешанной формы киберагрессивного поведения также используйте 3 памятку **Навигатора профилактики девиантного поведения (2022)**

Для работы с жертвами используйте 4 памятку по кибервиктимному поведению данного Навигатора и/или памятки **Навигатора профилактики виктимизации детей и подростков (2024)**

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**

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 объёмах, 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 психоэмоциальными 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 (груминг)

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/**