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.

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.

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.

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/**