МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОФИЛАКТИКЕ АКТУАЛЬНЫХ УГРОЗ ИНТЕРНЕТ-МОШЕННИЧЕСТВА СРЕДИ ОБУЧАЮЩИХСЯ

Оглавление

Введение

В современном мире цифровые технологии стремительно развиваются, и их доступность открывает для людей широкие возможности в сфере коммуникаций, образования, досуга, финансовых транзакций и многого другого. Однако эти же технологии становятся платформой для злоумышленников, которые создают и совершенствуют мошеннические схемы, используя все новые методы социальной инженерии, технических взломов и психологических уловок.

Наиболее распространённые виды мошенничества, с которыми сталкиваются пользователи интернета, включают:

- Фишинг: рассылка поддельных писем и сообщений с целью выманить у жертвы пароли, логины, данные банковских карт.
- Социальная инженерия: манипуляции и убеждение пользователя в том, что он обязан предоставить определённые сведения, совершить перевод денег или «выручить друга».
- Продажа/аренда аккаунтов: люди, в том числе несовершеннолетние, передают доступ к своим учетным записям (например, WhatsApp, «Госуслуги», банковские аккаунты) криминальным структурам, не осознавая серьёзности последствий.
- Ложные инвестиции и псевдообменники: схемы быстрого обогащения, где жертву привлекают высокими процентами дохода, но после внесения средств мошенники исчезают.

Эти формы мошенничества далеко не новы, но их масштабирование в цифровом пространстве, а также использование современных инструментов анонимности, криптовалют и глобальных сетевых сообществ сделали проблему острее, чем когда-либо.

Более того, постепенно меняются и методы вовлечения новых «кадров» для совершения противоправных действий: мошенники охотно привлекают несовершеннолетних, понимая, что дети более подвержены внушению, а также надеются на их неосознанность и кажущуюся анонимность в сети.

Из открытых источников и сообщений правоохранительных органов известно о случаях, когда подростки 14–17 лет активно включались в схемы продажи и аренды аккаунтов (WhatsApp, Telegram, «Госуслуги»). В одном из недавних эпизодов упоминается десятилетний мальчик, сдавший свой аккаунт в мессенджере за скромную плату. Хотя ребёнку и нет 14 лет, факт передачи аккаунта позволил преступникам совершить ряд мошеннических действий. В итоге родители вынуждены были общаться с полицией и оказываться в крайне неприятной ситуации.

Известны эпизоды в Санкт-Петербурге, Туле, Кемерово, Иркутской области и других регионах, где задерживали целые группы подростков, зарегистрировавших тысячи аккаунтов и продавших доступ к ним кураторам из украинских колл-центров. Такая деятельность квалифицируется как мошенничество и пособничество (ст. 159 УК РФ), в некоторых случаях — как кража (ст. 158 УК РФ) при похищении средств, в связи с чем МВД России уже задержан ряд подростоков.

Подростки и дети — наиболее уязвимая категория, так как они часто не обладают достаточным социальным и юридическим опытом, чтобы оценить последствия своих действий. Мошенники пользуются несколькими ключевыми факторами:

- Наивность и доверчивость: дети по природе своей легче доверяют взрослым, а если взрослый прикидывается «другом» или «куратором» в чате, он может быстро наладить контакт и выстроить псевдо-доверительные отношения.
- Желание быстрого заработка: экономический и социальный фон в подростковом возрасте часто формирует мечты о независимости и деньгах «здесь и сейчас». Мошенники умело эксплуатируют эту жажду легких доходов.
- Недостаток внимания со стороны взрослых: родители, перегруженные работой и жизненными проблемами, подчас слабо контролируют онлайн-активность своих детей.

- Недостаток цифровой грамотности: многие подростки умеют хорошо пользоваться смартфоном, мессенджерами, но при этом не осознают всех правовых и технических аспектов безопасности. Они могут с лёгкостью передать доступ к аккаунту, не понимая, что становятся соучастниками преступления.

Именно поэтому воспитательная и просветительская работа в сфере интернет-безопасности должна быть комплексной: необходимо задействовать классных руководителей, учителей информатики, ОБЗР, психологов, администрацию школы и, конечно, родителей. Без общего «фронта» усилий педагогической среды результат будет слабым.

По данным исследования федеральной инновационной площадки Минобрнауки России «Сетевичок», около 35% подростков отметили, что готовы довериться онлайн-знакомому, если он имеет общих друзей или выказывает «доброжелательное отношение». При этом почти четверть респондентов (24%) признались, что уже оказывались в ситуациях, когда незнакомые лица в сети пытались манипулировать их чувством долга или дружбы. Эти цифры наглядно демонстрируют важность формирования у учащихся критического мышления и устойчивости к социальному давлению, а также необходимости поддержки со стороны взрослых.

Многие педагоги изначально считают, что ответственность за цифровую безопасность и профилактику мошенничества лежит исключительно на учителях информатики или, в крайнем случае, ОБЗР. Но в реальности:

- Педагоги часто сами являются родителями. Даже если это не входит в круг их профессиональных обязанностей, они заинтересованы в безопасности собственных детей. Чем выше понимание проблемы у взрослых в школе, тем эффективнее и дома будет выстроена профилактика.
- Учителя любых предметов ежедневно взаимодействуют с детьми, ведут классное руководство, мониторят поведение учащихся. Именно они первыми замечают тревожные звоночки: изменение поведения, появление лишних денег, секретность, агрессивную реакцию на вопросы.
- Единичный случай — это проблема для всех: даже если всего один ученик столкнулся с серьёзным мошенничеством, оно может затронуть множество семей (например, если с его аккаунта будут рассылаться ссылки одноклассникам) или спровоцировать криминальную волну в школе.
- Воспитательная функция школы не ограничивается отдельным предметом. Любой педагог может (и должен) внести вклад: дать совет, провести небольшое

обсуждение на классном часу, предупредить коллег и родителей о возможных рисках.

Таким образом, участие педагогов в профилактике вышеуказанных рисков необходимо. Знания о цифровых ловушках позволят любому педагогу своевременно распознать проблему, принять меры или направить ребёнка к специалистам.

Правовая оценка интернет- мошенничества

В Российской Федерации существуют конкретные правовые нормы, регулирующие вопросы мошенничества и сопряжённой с ним деятельности.

Статья 159 УК РФ «Мошенничество» определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. В разных частях статьи уточняются квалифицирующие признаки (группа лиц по предварительному сговору, крупный размер, использование служебного положения и др.). Максимальное наказание может достигать 10 лет лишения свободы, в зависимости от тяжести и квалифицирующих обстоятельств.

Статья 158 УК РФ «Кража» может применяться, если действия связаны с тайным хищением имущества, в том числе путём незаконного использования чужих средств доступа к счетам или электронным кошелькам, а также может быть сопряжена с деяниями в интернете, если речь идёт, например, о хищении денег со счёта.

В случае передачи или сбыта похищенных данных могут применяться статьи, связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ) и т.д.

В тоже время, при использовании ребёнка в преступной деятельности — возможны дополнительные квалификации (ст. 150 УК РФ «Вовлечение несовершеннолетнего в совершение преступления»).

Однако, уголовная ответственность наступает с 16 лет по общему правилу, а по ряду тяжких преступлений с 14 лет (убийство, изнасилование, кража, грабёж, разбой, вымогательство, терроризм и др.). Мошенничество не входит в список статей, предусматривающих ответственность с 14 лет, но при наличии других составов (например, кражи) ответственность может наступить и раньше. Это означает, что подросток 14–15 лет может быть привлечён к ответственности, если деяние квалифицируется, например, как кража или вымогательство в составе группы преступлений. Кроме того, в ряде случаев может идти речь о вовлечении несовершеннолетнего (если кто-то старше 18 лет побуждал подростка участвовать в преступлении).

Родители часто не осознают, что могут быть привлечены к ответственности, если будет доказана их бездействующая или активная роль в преступлениях детей:

- Если родители способствовали действиям ребёнка, поощряли или предоставляли ресурсы (например, SIM-карты, банковские карты), в некоторых случаях их действия могут быть расценены как соучастие.
- Если ребёнок систематически совершает правонарушения, может быть поставлен на учёт в ПДН (подразделение по делам несовершеннолетних), а родители — привлечены к ответственности за неисполнение обязанностей по воспитанию.

Кроме того, моральные и социальные последствия колоссальны: помимо административных или уголовных мер к самому ребёнку, факты вовлечения в мошенничество могут создавать серьёзные проблемы в дальнейшем обучении, поступлении в вузы и трудоустройстве.

Основные схемы вовлечения детей в мошенничество

Самая масштабная площадка — Telegram, где нередки анонимные каналы, посвящённые продажам аккаунтов, SIM-карт, баз данных. Мошенники создают тематические группы и чаты, куда приглашают или сами добавляют подростков. Там публикуются объявления: «Куплю аккаунт WhatsApp за 200 рублей», «Нужны люди с SIM-картами МТС для работы».

Подросткам внушают, что это «серое» дело, где «никого не поймают». Для привлечения используются «яркие картинки», обещания лёгкой прибыли и анонимности. Как правило, реальность другая: правоохранительные органы активно мониторят подобные каналы, а конечная выгода для ребёнка минимальна, но риски громадны.

Второй популярный инструмент — WhatsApp. Иногда мошенники работают напрямую, рассылая сообщения с незнакомых номеров, предлагая «простой заработок» за передачу учётной записи. Достаточно сказать «да», сообщить шестизначный код, и аккаунт переходит в руки злоумышленника.

Многие дети — заядлые геймеры. Они часто общаются в Discord, внутриигровых чатах (например, в Fortnite, Roblox, Minecraft и пр.). Именно там могут появляться «предложения» купить виртуальную валюту по сниженной цене, ввести промокод, перейти на сторонний сайт и «зарегистрироваться» для получения бонуса. Под видом этих действий подростков просят скинуть личные данные, выполнить «легкую работу» (сдать аккаунт, оформить фейковую учётную запись), а затем используют их реквизиты в преступной схеме.

Соцсети по-прежнему остаются популярным местом для подростковой активности. Там есть закрытые и полузакрытые группы, куда приглашают «для заработка», «для совместного бизнеса» и т.д. Часто это выглядит как MLM (сетевой маркетинг) или финансовая пирамида, но внутри скрывается преступная схема.

Например, нередко используют истории успеха: «Этот школьник 15 лет заработал 50 тысяч, просто продавая доступ к аккаунту WhatsApp!». Подростки заражаются энтузиазмом, хотят повторить «успех». На деле же часто остаются и без обещанной суммы, и с перспективой разговора в полиции.

На «Авито» и аналогичных ресурсах выложить объявление о продаже SIM-карт, аккаунтов или каких-то документов может любой желающий. Подростки видят: «Покупаем аккаунты недорого». Связываются с продавцами, передают данные, и уже становятся частью цепочки.

Опасность с «Госуслугами» в том, что получение доступа к чужому профилю даёт мошенникам огромный спектр возможностей: от оформления электронных подписей до подачи заявлений и получения выплат.

В теневом сегменте интернета или в закрытых чатах существует множество форумов, где инструкции по мошенничеству циркулируют свободно. Доступ туда часто продаётся за небольшие деньги, и подростки, увлечённые «хакерской романтикой», платят за вход. Внутри они получают подробные руководства и «техподдержку» от более опытных мошенников.

Для регистрации в большинстве вышеуказанных сервисов и мессенджеров требуется номер телефона. При активации аккаунта система отправляет на него SMS с кодом подтверждения. Тот, кто вводит код, получает доступ. Таким образом, любая передача SIM-карты или кода подтверждения фактически означает передачу управления учётной записью.

Опасность в том, что со сданного в аренду аккаунта затем совершаются звонки гражданам от имени «сотрудников банка» или «правоохранительных органов». При этом все действия осуществляются под вашим именем или номером. Впоследствии следы приводят к владельцу SIM-карты, что означает большие проблемы с законом, поскольку в дальнейшем реализуются различные мошеннические схемы:

- Фишинг: злоумышленник создаёт поддельную страницу, копирующую внешний вид «Госуслуг», банка или соцсети. Человек вводит логин/пароль, и они попадают к мошенникам.

- Взлом аккаунтов: используются уязвимости, простые пароли, утечки баз данных. Часто взломанные аккаунты затем продаются или используются для дальнейших мошенничеств.
- Подмена телефонных номеров: существуют сервисы, позволяющие звонить с «подставного» номера (например, официального номера банка). Подростки, вовлечённые в схему, могут использовать подобные инструменты, думая, что их невозможно отследить. На самом деле правоохранители обладают средствами установления реального источника звонка.

В этой связи, как дети, так и родительская и педагогическая общественность должны быть осведомлены о базовых принципах информационной безопасности:

- Необходимо использовать сложные пароли и двухфакторную аутентификацию;
- Необходимо использовать антивирус и осуществлять регулярные обновления программного обеспечения.
- Использование нелицензионных программ повышают риски взлома;
- Необходимо осторожно обращаться с сообщениями от незнакомых контактов и ссылками.

Психологические аспекты вовлечения подростков

Важно отметить, что дети младшего школьного возраста (7–10 лет) также подвержены интернет-угрозам, хотя механизм вовлечения отличается от подросткового. На данном этапе развития доминируют наглядно-действенное мышление, повышенная внушаемость и доверчивость к взрослым, особенно в онлайн-среде, где дети не всегда способны отличить реального собеседника от вымышленного. Эмоциональная незрелость и отсутствие критического мышления делают младших школьников крайне уязвимыми к манипулятивным схемам — от навязывания «дружбы» до вовлечения в обмен данными.

В подростковом возрасте дети часто испытывают острое желание самоутвердиться, иметь «свои» деньги для покупки одежды, гаджетов или развлечений. В социальных сетях и мессенджерах подростки натыкаются на яркие объявления: «Лёгкие деньги без вложений!», «Поделись номером и заработай!», «Анонимно и безопасно», «Куратор сам всё сделает, тебе только надо дать код». Дети, неопытные в вопросах сетевых афер, легко поддаются искушению.

С психолого-педагогической точки зрения подростковый возраст (11–17 лет) представляет собой критический этап развития личности, характеризующийся

становлением Я-концепции, повышенной чувствительностью к оценке окружающих и стремлением к независимости. Согласно концепции Э. Эриксона, подросток находится в стадии «идентичности против ролевой растерянности», где формирование собственной позиции часто происходит через эксперимент, в том числе с социальными нормами. Отмечается также высокий уровень потребности в принадлежности к группе, что делает подростков особенно восприимчивыми к давлению со стороны сверстников и привлекательным образам «успешных ровесников». Недостаточно сформированные волевые регуляции и переоценка собственных возможностей способствуют принятию рискованных решений, в том числе в цифровой среде.

Важнейший фактор в указанных обстоятельствах — групповое давление и стремление быть «как все» или даже «круче всех». Если в компании несколько подростков уже занимаются мошеннической деятельностью, то они могут вовлекать других, рассказывая о быстрых и простых деньгах. Пытаясь не отставать, ребёнок соглашается, не успев задуматься о последствиях. Для подростков статус в группе часто важнее родительских предостережений. Особенно если родители не имеют авторитета или не вникают в жизнь своих детей, а в школе нет систематической профилактической работы.

При этом, дети и подростки с низкой самооценкой, конфликтами в семье, чувством одиночества могут искать признания и поддержки на стороне. Интернет и мессенджеры дают иллюзию принятия, а мошенники в роли «доброжелательных наставников» предлагают якобы безобидные задания: «Передай код», «Зарегистрируй аккаунт». Постепенно задания усложняются, ребёнок уже втягивается в криминальную сеть и боится отказаться.

Таким образом, педагог, находящийся с детьми в постоянном контакте, может заметить:

- Изменения в эмоциональном фоне и поведении. Если ранее спокойный ребёнок вдруг становится раздражительным, скрытным, тревожным или, наоборот, проявляет нездоровую эйфорию от обсуждения денег и заработка в сети, это может говорить о том, что он столкнулся с манипуляциями мошенников или испытывает внутренний конфликт из-за сомнительных действий.
- Новые социальные контакты и необычное окружение. Подросток может вступать в незнакомые онлайн-сообщества, добавлять в друзья сомнительных контактов или постоянно переписываться с людьми, о которых ничего не известно.

- Резкое изменение отношения к деньгам. Если ученик внезапно начинает сильно интересоваться деньгами, быстрыми заработками, хвастается новыми покупками без ясного источника средств, либо, наоборот, проявляет повышенную тревогу по поводу финансов, стоит проверить, не вовлечён ли он в мошеннические схемы или «легкие подработки» в интернете.
- Нарушение самооценки и внушаемость. Дети, имеющие низкую самооценку или стремящиеся к признанию любой ценой, могут особенно остро реагировать на лесть, обещания высокого статуса или «уникальных возможностей» заработать, которые предлагают мошенники.
- Косвенные проявления манипуляций. Подросток может стать скрытным: уходит в другую комнату для переписки, быстро сворачивает экран при приближении взрослых, не даёт смотреть на свой телефон или агрессивно реагирует на попытки обсудить его активность в сети.

Организация профилактики

Профилактика вовлечения обучающихся в мошеннические схемы, в том числе с использованием цифровых технологий, входит в сферу ответственности образовательной организации в соответствии с требованиями Федерального закона № 273-ФЗ «Об образовании в Российской Федерации», а также положениями ФГОС и ФООП:

- В требованиях ФГОС обозначено, что система воспитания должна обеспечивать формирование у обучающихся ответственного и безопасного поведения в информационной среде;
- Программами воспитания предусмотрены направления работы по профилактике асоциальных явлений и правонарушений среди несовершеннолетних, включая риски в цифровом пространстве.

Классный руководитель часто является центральной фигурой в воспитательном процессе. Не зависимо от уровня своей цифровой компетентности, ему важно:

- Освоить базовую терминологию: что такое мессенджер, фишинг, SIM-карта, аккаунт.
- Знать «тревожные звоночки»: изменения в поведении, резкое появление денег, секретность.
- Проводить регулярные короткие беседы с классом о безопасном поведении в сети.

- Поддерживать связь с родителями: держать их в курсе замеченных изменений, предоставлять им простые памятки.

Учителя информатики, ОБЗР и другие специалисты, обладающие необходимой подготовкой, могут глубже раскрыть вышеуказанные вопросы. На каждом учебном предмете и для любой возрастной группы можно найти формат занятий или заданий, позволяющий повысить бдительность детей к онлайн-рискам, не посвящая их в «технологии» противоправных действий.

Ключевые принципы при подборе заданий:

- Возрастная доступность: чем младше ребёнок, тем проще и нагляднее форма работы (картинки, короткие истории). Старшим можно давать элементы ролевых игр и анализа реальных кейсов.
- Отсутствие «рецептов»: не объяснять «как» совершаются преступные действия, а показывать, почему это опасно и незаконно.
- Акцент на выборе: ребёнок должен понять, что всегда есть возможность отказаться или посоветоваться со взрослыми.
- Правовой и моральный контекст: подчёркивать, что даже «малая» помощь мошенникам — это реальное нарушение закона и удар по собственной репутации.

В начальной школе (7–10 лет) можно провести урок чтения или окружающего мира, где детям предлагается прочитать короткий рассказ или диалог, в котором один персонаж пытается выведать у другого какую-то личную информацию, например пароль от игры или номер телефона. После чтения учитель организует обсуждение, задавая вопросы о том, что может произойти, если главному герою поверят, к кому следует обратиться, если подобная просьба исходит от незнакомца, и как отличить безопасный запрос от опасного. Цель такого занятия — выработать у учащихся младшего звена установку «Не делиться личными данными с незнакомцами, обо всём рассказывать родителям или учителю».

В рамках урока рисования (ИЗО) в той же возрастной группе можно предложить детям тему «Мой безопасный интернет». Ребята рисуют плакат или эмблему, где отражают правила безопасного поведения в сети, например призывы вроде «Не передавай коды, не сообщай пароль», а педагог при этом демонстрирует несколько понятных «иконок-символов» вроде замка или знака «стоп». Важно не вдаваться в подробности мошеннических схем, а лишь укреплять у детей ассоциации с правильным и осторожным пользованием интернетом.

В среднем звене (10–14 лет) на уроках русского языка или литературы может быть проведено задание по анализу небольшого псевдо-рекламного текста, где обещают лёгкий заработок в обмен на номер телефона и код из SMS. Ученики должны найти в этом тексте сомнительные выражения, распознать возможный обман и сформулировать, как поступил бы человек, заботящийся о своей безопасности. Такая работа способствует критическому чтению и учит ребят настораживаться при виде подозрительных «выгодных» предложений.

На уроках математики этого же звена целесообразно обсудить финансовые обещания, которые явно выходят за рамки разумных показателей, например предложение увеличить вклад в пять раз за неделю. Подростки смогут посчитать, какой процент доходности это предполагает, и сделать вывод, что столь высокий рост капитала обычно связан с мошенническими схемами. Важно подчеркнуть, что задача демонстрирует лишь «подозрительность» подобных обещаний, не раскрывая способов обмана.

На уроках обществознания или ОБЗР учитель может напомнить, что подросток, отдавший доступ к своему аккаунту за деньги, рискует нарушить закон. Вопросы об уголовной и административной ответственности, о причинах, по которым «Я не знал» не снимает вины, помогут сформировать представление об ответственности за поступки, совершённые в сети, без углубления в конкретные способы обмана.

В старшей школе (15–18 лет) учителям информатики стоит сосредоточиться на вопросах безопасности аккаунтов и личных данных: можно показать типовые настройки мессенджера (двухфакторная аутентификация, скрытие номера телефона) и дать учащимся проверить, насколько надёжно настроен их собственный профиль. Это помогает понять, как легко злоумышленники могут получить доступ к приватным сведениям, если пользователь сам не заботится о защитных мерах. При этом не требуется детально объяснять, как именно «ломают» аккаунты, достаточно продемонстрировать пользу элементарных предосторожностей.

Учителя литературы или русского языка старших классов могут предложить анализ текстов, в которых авторы (мошенники) используют эмоциональную манипуляцию: лесть, запугивание, обещания быстрого выигрыша. Главная цель здесь — научить старшеклассников распознавать речевые приёмы, провоцирующие доверие, и формулировать грамотный ответ, который позволяет не поддаваться на уловки. На уроке права или обществознания (углублённый уровень) стоит упомянуть недавние инициативы по ужесточению наказания за передачу платёжных инструментов третьим лицам. На примере кейса, где подросток «просто дал карту приятелю», можно обсудить принцип

«Незнание закона не освобождает от ответственности» и выяснить, что стоит предпринять, если друзья предлагают поучаствовать в схеме «лёгкого заработка».

Для любого возраста существует ряд общих идей. Например, можно вместе с детьми составить проект «Карты безопасных ресурсов», где ученики найдут и запишут адреса надёжных порталов, таких как официальные сайты банков или «Госуслуг», и научатся отличать оригинальные доменные имена от фальшивых, используемых во фишинговых атаках. Кроме того, педагоги нередко упоминают «Правила 3 „Не“»: не сообщать пароли или коды из SMS, не переводить деньги без проверки, не устанавливать программы и приложения из неизвестных источников. Полезно и дать ученикам задание сделать для родителей короткую памятку: три-четыре простых принципа интернет-безопасности, и попросить взрослых оставить в дневнике или на отдельном листе подпись о том, что они ознакомлены с этими советами.

Школьные психологи могут проводить не только стандартные консультации, но и целый комплекс превентивных мероприятий, направленных на раннее выявление признаков, указывающих на возможное вовлечение подростков в преступные схемы. Школьный психолог организует несколько форм работы:

Групповые тренинги, посвящённые теме манипуляции, давления и убеждения. На таких занятиях подростки учатся распознавать психологические приёмы, которыми мошенники вызывают доверие (лесть, запугивание, псевдо-дружелюбие), и получают базовые навыки противостояния манипуляциям. Важно, чтобы тренинг не содержал конкретных инструкций о том, как совершается преступление, а фокусировался на развитии личностной устойчивости и критического мышления.

Индивидуальные консультации с учащимися, проявляющими признаки вовлечения в мошеннические схемы или демонстрирующими повышенную тревожность и склонность к риску. Психолог выстраивает доверительную беседу, стараясь понять, что именно привлекает ребёнка в сомнительных предложениях, и даёт рекомендации, как безопасно удовлетворить потребность в признании, финансовой самостоятельности или новых впечатлениях.

Родительские лекции и семинары, во время которых психолог разъясняет взрослым, как заметить «красные флажки» в поведении ребёнка, как выстроить доверительные отношения без постоянных конфликтов и упрёков, а также как вовремя выявить склонность подростка к риску или попаданию под чужое влияние. Подчёркивается необходимость

деликатного контроля и живого интереса к жизни ребёнка, а не только формальной проверки гаджетов.

Помимо этого, психологу важно наладить тесное взаимодействие с социальным педагогом, особенно когда речь идёт о детях из социально уязвимых категорий, воспитанниках интернатов, семьях с низкой вовлечённостью родителей. Социальный педагог может:

- Осуществлять контакт с органами опеки и профильными организациями, если ребёнок фактически лишён родительского надзора.
- Помогать в организации профилактических мероприятий в школе, координируя работу классных руководителей, чтобы те при необходимости вовремя сигнализировали о тревожных изменениях в поведении детей.
- Проводить беседы и консультации, в ходе которых выясняет социальные условия жизни ученика (финансовое положение семьи, наличие свободного времени, эмоциональная поддержка) и при необходимости предлагает пути решения — например, вовлечение ребёнка в кружки или проекты, которые повысят его самооценку и отвлекут от желания «заработать» сомнительным способом.

Администрация образовательной организации несёт общую ответственность за профилактику правонарушений и должна:

- Организовать внутришкольные правила и регламенты относительно использования мобильных телефонов в урочное время, проверок на наличие запрещённых действий в сети (без нарушения прав детей).
- Создать систему взаимодействия с правоохранительными органами (ПДН, киберполиция), чтобы при необходимости оперативно реагировать на факты вовлечения детей в криминал.
- Проводить собрания и совещания, где педагоги могут делиться наблюдениями, проблемами и успехами в профилактике.

Возможности организации профилактики вне образовательной организации

Эффективная профилактика мошенничества среди школьников может быть организована в рамках внеклассных мероприятий и домашних заданий, включая периоды каникул. Помимо традиционных форм внеурочной работы, таких как конкурсы,

киберквесты или ролевые игры, следует учитывать сезонные риски и особенности нагрузки на учеников.

Так, во время продолжительных каникул дети чаще пользуются смартфонами и социальными сетями, что увеличивает их уязвимость перед различными схемами мошенничества. Поэтому целесообразно заблаговременно давать учащимся специальные задания на каникулы, например: подготовить мини-презентации или эссе на тему «Как я защищаюсь от обмана в интернете», собрать и представить классу историю о новом типе мошенничества, замеченном ребёнком или его близкими, или провести небольшой анализ настроек безопасности собственного смартфона и социальных сетей, сделав скриншоты и составив чек-листы.

Также эффективным методом профилактики является проведение специальных онлайн-активностей («летних челленджей»). Например, акция «Безопасное селфи» может помочь детям понять, какие персональные данные (номер телефона, домашний адрес, паспортные данные и т.п.) категорически нельзя публиковать. Другая акция — «Расскажи родителям» — направлена на то, чтобы дети сами объясняли старшим родственникам основные правила безопасности в интернете, что значительно укрепляет собственные навыки учащихся.

Не менее важна организация постоянной обратной связи по вопросам безопасности. Для этого школа может создать специальный чат или раздел в школьном мессенджере, куда учащиеся могли бы обращаться за консультациями в период каникул, получая своевременные рекомендации от педагогов или назначенных кураторов. Родителей, в свою очередь, следует побуждать сообщать школе через электронный дневник или чат обо всех подозрительных случаях, произошедших с детьми за период каникул.

Дополнительно, рекомендуется разместить в электронном журнале или на официальном сайте школы перечень полезных ссылок и памяток, посвящённых теме кибербезопасности (например, ссылки на ресурсы МВД или профильные порталы), указав на важность их изучения до начала нового учебного года.

При работе с реальными ситуациями из новостей («кейсы») важно представлять их таким образом, чтобы не раскрывать учащимся технологические детали преступлений. Преподавателю следует формулировать эти кейсы нейтрально и кратко, избегая информации, которая могла бы быть использована подростками в противоправных целях. Например, учитель может взять новостную заметку о задержании подростков, вовлечённых в мошенническую схему (передача SIM-карт или аккаунтов третьим лицам), и представить

её учащимся в сокращённой форме. В таком кейсе должно сообщаться только о факте нарушения закона и его последствиях, без указания технических деталей мошеннической схемы.

В ходе обсуждения таких кейсов основной упор делается на морально-этические и правовые аспекты проблемы: почему подростки могли посчитать подобное предложение безобидным, в чём главная опасность подобной деятельности, а также как правильно поступить, если учащийся столкнулся с подобным предложением (например, сообщить родителям или отказаться). При этом важно категорически избегать обсуждения технических ошибок преступников или способов их исправления, чтобы не провоцировать интерес к преступным схемам.

Взаимодействие с родителями

Не все родители разбираются в технологиях: кто-то едва умеет пользоваться смартфоном, кто-то не понимает принципов работы «Госуслуг». При этом дети намного продвинутее технически, что создаёт дезориентацию. Задача школы — донести базовые основы:

- Как проверить настройки телефона ребёнка?
- Почему нельзя передавать SIM-карту и пароли?
- Какие виды мошенничества существуют?

Главный инструмент профилактики — доверительные отношения в семье. Если подросток чувствует, что может в любой ситуации обратиться к родителю за советом и не будет немедленно наказан или высмеян, шанс вовлечения в мошенничество снижается.

Рекомендации по контролю и поддержке цифровой активности детей:

- Установление разумных правил: где и сколько времени ребёнок может проводить в сети, как и какие данные разрешено публиковать.
- Регулярные беседы: обсуждать новости о мошенничестве, совместно смотреть обучающие ролики о безопасности.
- Технический контроль: антивирус, родительский контроль на уровне роутера или ОС (но без тотальной слежки, которая может вызвать протест).

Родительские собрания и индивидуальные консультации — важная часть профилактики. Нужно объяснять, что никакие технические фильтры не заменят живого общения и взаимного доверия. Родителям полезно дать простые рекомендации (чек-лист):

- Проверяйте, где регистрируется ребёнок, какие приложения устанавливает.
- Разговаривайте об источниках денег, появляющихся у подростка.
- Учитесь вместе с ребёнком цифровой грамотности, смотрите обучающие ролики.

По итогам опроса, проведённого федеральной инновационной площадкой Минобрнауки России «Сетевичок», лишь 28% родителей имеют чёткое представление о том, какие приложения и чаты посещает их ребёнок, а свыше 45% не могут назвать ни одного официального ресурса по вопросам кибербезопасности. Подобный недостаток осведомлённости тормозит профилактические усилия школы и подчёркивает потребность в систематическом взаимодействии с семьёй.

Однако существует категория учащихся, которые не могут рассчитывать на семейную поддержку, в том числе дети-сироты и воспитанники интернатов, а также дети, чьи родители по разным причинам не уделяют должного внимания воспитанию. В таких случаях роль школы и педагогов вырастает многократно. Именно учитель или психолог может стать для подростка единственным «взрослым доверия», к которому он обратится за помощью. Главная задача педагогов в подобных случаях — вовремя заметить уязвимость и взять инициативу по оказанию помощи, не полагаясь на бездействующих родителей. Инициирование профилактических мер — в том числе координация с правоохранителями, психологами, общественными организациями — способно защитить ребёнка от пагубного влияния мошенников и дать ему ощущение, что он не одинок в решении своих проблем.

Алгоритм действий педагога при выявлении фактов вовлечения обучающихся в мошеннические действия

В первую очередь, общение с ребёнком должно быть спокойным и доверительным. Не стоит угрожать или давить. Цель — получить информацию: какие ресурсы, кто пригласил, что именно делал ребёнок. Желательно записать контактные данные, каналы, никнеймы, если это безопасно и возможно.

Далее необходимо проинформировать классного руководителя (или, если вы и есть классный руководитель, — администрацию) и вызвать родителей для индивидуальной беседы.

Если есть подтверждение, что ребёнок уже участвовал в незаконных действиях, нужно действовать по внутреннему регламенту школы и законодательству РФ. Возможно, потребуется письменное заявление или обращение к соответствующим органам (МВД России).