Выписка из протокола педагогического совета
МАОУ «Школа №45 с углубленным изучением отдельных предметов»
ГО г.Уфа РБ №24 от 28.08.2026 г

Повестка:

3. Информационная безопасность подростков в современной агрессивной цифровой среде.

По третьему вопросу выступил заместитель директора по ВР Васюк Д.А.

Дети и подростки – активные пользователи интернета как в мире, так в РФ.

Доступ несовершеннолетних к сайтам в сети Интернет дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимая в них участие, и использовать сеть Интернетв качестве источника для собственного развития.

Однако использование сети Интернет вместе с возможностями несет и различные риски.

В Концепции ИБ приведены риски, которым подвержены дети в области виртуальной

коммуникации дети:

– стать жертвой компьютерного мошенничества и вымогательства;

– вовлечение в сексуальную эксплуатацию, террористическую и экстремистскую деятельность;

– распространение наркотических средств, психотропных веществ и их прекурсоров, аналогов наркотических средств и психотропных веществ и новых потенциально опасных

психотропных веществ посредством игровых активностей;

– вовлечение в сообщества с нарушением общепринятых норм морали;

– прочтение детьми информации, вредящей их мировоззрению и психотическому состоянию.

Современные дети, в отличие от предыдущего поколения, имеют более широкий доступ к средствам компьютерной техники (планшеты, мобильные телефоны, компьютеры с подключенным домашним, мобильным интернетом или точки доступа по wi-fi в общественных местах). При этом многократно возросла нагрузка на нервную систему подростка, а перспектива остаться вне информационного потока вызывает сильную тревогу.

Опасности для детей и подростков в сети Интернет:

1. Вовлечение в опасные группы и движения

В соответствии с Концепцией ИБ, на сегодняшний день широкое распространение в цифровой среде получили деструктивные молодежные субкультуры, включая движения, связанные с вооруженным нападением на образовательные организации, популяризацией деятельности криминальных сообществ, продвижением преступных и антиобщественных действий, в том числе агрессивного, насильственного, суицидального, экстремального и экстремистского характера.

Все большее распространение получает задействование сетевых платформ и мессенджеров для вовлечения детей в несогласованные публичные мероприятия (включая протестные акции), поскольку несовершеннолетние не только легче поддаются идеологическому и психологическому воздействию, но и при определенных обстоятельствах не подлежат уголовной ответственности.

Вовлечение подростков в группы деструктивной направленности очень часто происходит через Интернет:

– социальные сети и информационные порталы («ВКонтакте»; «Фейсбук»*, «Инстаграм»* (*запрещены на территории Российской Федерации) и т.п.);

– Интернет-сообщества, тематические форумы, шок-контент (например, «Привет со дна», «Группа смерти» и др.);

– Интернет-игры (например, «Большая игра. Сломай систему!» и др.).

Общие маркеры вовлечения обучающихся в деструктивные группы:

– изменение внешности;

– изменение эмоционального состояния и его неустойчивость;

– преобладание в мировоззрении обучающихся идей неравенства, дискриминации, возмездия и наказания за несправедливое отношению;

– агрессивное поведение;

– использование сленга, относящегося определенной деструктивной идеологии;

– смена привычного образа жизни;

– безразличие к учебной, групповой и общественно-полезной деятельности;

– скрытность в отношении ежедневной занятости и планов;

– систематические пропуски учебных занятий по неуважительной причине.

Общие маркеры вовлечения обучающихся в деструктивные сообщества сети Интернет:

– резкое изменение данных личного профиля в социальных сетях;

– подписка на группы и сообщества, посвященные деструктивной идеологии или движению;

– публикация и репостинг материалов, отражающих содержание идей деструктивного

сообщества (группы);

– публикация статусов, выражающих агрессию или содержащих отсылку к деструктивному движению;

– новые «друзья» в социальных сетях, разделяющие интерес ребенка к деструктивной идеологии («понимающие» его);

– ограничение доступа всех близких к личному Интернет – аккаунту.

Профилактическая работа с обучающимися по вопросам избегания вовлечения в опасные группы и движения:

– социально-педагогическая диагностика обучающихся;

– психологическая диагностика особенностей психоэмоционального состояния и личностных особенностей обучающихся;

– проведение разнообразных дискуссий, диспутов с несовершеннолетними;

– проведение деловых игр с целью выявления интересных и социально-значимых занятий;

– проведение психологических тренингов, циклов занятий, направленных на формирование и развитие толерантности;

– вовлечение в разнообразную организованную досуговую деятельность с учётом индивидуальных особенностей, способностей и потребностей обучающихся;

– вовлечение в детские и подростковые социальные проекты, направленные на включение школьников в социально-ориентированное творчество, на развитие их гражданской ответственности перед окружающим миром;

– межведомственное взаимодействие с субъектами профилактики.

2. Кибербуллинг

Кибербуллинг – различные формы травли, где агрессор и жертва встречаются в сети Интернет. Чаще всего пострадавшими становятся дети и подростки как самая уязвимая категория пользователей. Подросток, ставший объектом повышенного негативного внимания, испытывает на себе все «прелести» буллинга – уничижительные комментарии, оскорбления в сообщениях через мессенджеры, высмеивание в группах социальных сетей.

Механизмы травли в реальности и травли в сети «интернет» похожи, но кибербуллинг опаснее тем, что может происходить круглосуточно, от него не скроешься и не уйдешь домой.

В социальных сетях легко привлечь к процессу кибербуллинга большое количество последователей, распространив пост соответствующего содержания. Современным подросткам достаточно бросить клич в аккаунте, разместить фото и контакты объекта травли, регулярно поддерживать негативное отношение к нему записями на стене и так далее. Помимо прямых оскорблений в адрес жертвы, формой буллинга могут быть

выложенные на всеобщее обозрение личные фото, фрагменты переписок, мемы, созданные на основе изображения человека, и др.

Подростковый кибербуллинг особенно опасен тем, что его инициаторы в силу возраста не способны оценить, какой вред могут нанести их действия. То, что агрессивно настроенным школьникам представляется невинной шалостью, нередко становится причиной трагических и даже летальных исходов.

Методы борьбы с кибербуллингом:

– игнорировать нападки – следует объяснить обучающимся необходимость сдерживать эмоции, не вступать в перепалку с человеком, который явно хочет спровоцировать на ответную грубость;

– не винить себя - многие несовершеннолетние склонны искать причину агрессивного поведения оппонента в себе: что я не так сказал, чем я вызвал волну негатива? Следует объяснить обучающимся, что лично они тут ни при чем – пользователю-агрессору все равно, с кем затеять свару;

– исключить вероятность общения – необходимо создать условия, при которых инициатор кибербуллинга не сможет продолжать свои действия: внести его в черные списки, поставить запрет на поступление звонков и сообщений с его номера, а также писем с его электронных адресов;

– поделиться проблемой - кибербуллинг для подростков часто становится невыносимым испытанием, потому что им не с кем разделить свои переживания. Следует объяснить обучающимся, что если они не могут рассказать об этом родителям, можно позвонить в анонимную службу психологической поддержки: специалист внимательно выслушает, успокоит и даст дельный совет;

– бороться за свое спокойствие - травля в Интернете – явление распространенное, поэтому администрации соцсетей уже выработали алгоритм действий в случае жалоб на действия агрессивных пользователей. Они могут заблокировать профили, модерируют фотографии и посты, отслеживают появление комментариев с грубыми выражениями. Если дело дошло до угроз и клеветы, жертва кибербуллинга имеет все основания обратиться в полицию;

– дать отпор инициатору травли - агрессор рассчитывает, что жертва буллинга будет оправдываться, отвечать на его выпады колкостями, то есть поддаваться на провокации.

Любая другая реакция собьет его с толку. Следует объяснить обучающимся, что лучше сразу заявить о своем намерении обратиться в суд с иском о клевете и угрозах – это может подействовать отрезвляюще;

– соблюдать цифровую диету - радикальный способ избавиться от виртуального преследования – полностью отказаться на время от социальных сетей. Следует объяснить обучающимся, что можно на время удалить приложения из телефона, переключиться на приятные дела в реальной жизни;

– изменить поведение в сети - если предыдущий способ не подходит, следует пересмотреть свое отношение к интернет-ресурсам: ограничеть количество пользователей, которым доступен размещаемый контент, удалить фотографии, которые могут спровоцировать травлю, и так далее;

– соблюдать правила цифровой грамотности - следует объяснить обучающимся необходимость защиты личного киберпространства при помощи регулярно сменяемых сложных паролей; не стоит переходить по сомнительным ссылкам или устанавливать непроверенные приложения.

3. Домогательство, педофилия, завладение личной информацией или материалами с целью шантажа. В настоящее время во всем мире наблюдается устойчивый рост преступлений связанных с сексуальным насилием, изготовлением и распространением порнографии, в том числе детской. Детская порнография стала более распространенной и доступной благодаря развитию СМИ и интернет-ресурсов.

Не только детям, но и взрослым следует внимательно оценивать изображения, которые они выкладывают в Сеть. Многие считают, что при общении в Интернете их никто не найдет и не увидит. Главная угроза в том, что приватные фотографии, видео или сообщения могут стать не столь приватными.

Случается, что социальные сети в корыстных целях используют злоумышленники:

– педофилы, которые, ищут новые жертвы, выдавая себя за сверстника, искать личной встречи;

– мошенники, которые пользуясь доверчивостью подростков, выведывают конфиденциальную информацию;

– злоумышленники могут получить доступ к облачному хранилищу, куда автоматически отправляется медиаконтент со смартфона;

– подросток может потерять смартфон или забыть его в общественном месте – подобравший телефон посторонний человек может получить доступ к медиафайлам;

– опасность невольно может исходить даже от знакомых людей - человек, которому отправили сообщение, может выложить фотографии в Интернет или переслать друзьям.

Попав в чужие руки, эротические фотографии или видео могут стать инструментом шантажа. Кроме того, подобные материалы, размещенные в социальных сетях, могут «перекочевать» на порносайты.

Педагогу следует обсудить с обучающимися, насколько может быть опасно отправлять личные, а тем более — интимные фото и видео, с помощью которых можно установить, где и с кем живет ребенок, где и в какое время часто бывает.

В рамках занятий по интернет-безопасности нужно объяснить обучающему основные правила:

– не публиковать в социальных сетях информацию, по которой твое местонахождение

можно узнать (адрес, номер школы и др.);

– не нужно часто «чекиниться», то есть проставлять привязки к месту действия, выкладывая фотографии;

– держать страницу закрытой, в настройках разрешить отправку сообщений только друзьям и друзьям друзей;

– не идти на контакт с незнакомцами (и помнить, что даже за безобидной страницей сверстника может скрываться педофил);

– не встречаться в реальности с незнакомцами из социальных сетей; обсудить с ребенком возможные угрозы и опасности от встреч и онлайн-общения с незнакомцами и договориться о том, как он будет вести себя в той или иной ситуации;

– не высылать никому материалы, которые можно использовать для шантажа (например, пикантные фото, по которым тебя легко опознать);

– провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, доверять сведения личного характера человеку, которого никогда не видел вживую – разъяснить обучающимся, что в Интернете человек может представиться кем угодно;

– рекомендовать подросткам не рассказывать в Сети ничего такого, чего они могут стесняться;

– отказывать нормально; не нужно бояться обидеть собеседника, если он просит сделать что-то неприятное для тебя;

– создавать сложные пароли, различные для каждой социальной сети и электронной почты. Хранить пароли в надежном месте. Менять их с периодичностью 2-3 месяца.

Настроить двухэтапную аутентификацию;

– обращаться за помощью, если не справляешься с ситуацией. Как и во всех предыдущих ситуациях, крайне важно поддерживать атмосферу доверия в отношениях.

Инструменты шантажа и манипуляции работают тогда, когда понимание того, что о ситуации кто-то узнает (родители, учителя, одноклассники), вызывает у подростка ужас.

4. Кража паролей/аккаунтов в социальных сетях или играх Социальные сети и онлайн-игры стали настоящей пропиской современных детей. В социальных сетях они заводят друзей, общаются, делятся информацией, выкладывают фото и видео.

В онлайн-играх дети уделяют своим виртуальным героям много времени, «прокачивают» их, скупают «игровой шмот» за реальные деньги, которые дают родители, и страшно переживают, если с их аккаунтом что-то случилось.

Воровство паролей в социальных сетях и онлайн-играх явление достаточно распространенное, как результат можно потерять аккаунт и деньги, имеющиеся на привязанной SIM-карте или карте банка.

Судя по уже существующей в сети Интернет информации, чаще всего жертвы (дети 6-14 лет) сами сообщают свой пароль злоумышленникам, или мошенник заманивает пользователя на фишинговую страницу, предлагая ввести пароль с целью получить дополнительно игровые бонусы или привязать различные «фишки» к своей странице «ВКонтакте». Как только ребенок вводит пароль, его аккаунт немедленно крадут, а с ним зачастую и все деньги, имеющиеся на SIM-карте.

В рамках занятий по интернет-безопасности можно объяснить обучающему как защитится от кражи личных данных:

– рассказать о типах почты, которую могут рассылать злоумышленники, включая рекламу кредитных карт, необъяснимые товары и уведомления о сборе средств;

– рассказать о важности сохранения личной информации, такой как фамилии, адреса и номера телефонов, в тайне при обмене информацией в интернете;

– информируйте детей о нежелательных мошенничествах по электронной почте, таких как «фишинговые» электронные письма, в которых запрашивается личная информация, объясните, что лучше сразу удалять мошеннические электронные письма такого рода;

– провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, отвечать на различные наводящие вопросы, переходить по заманчивым ссылкам.

5. Интернет-зависимость от социальных сетей, сетевых игр, «серфингом», онлайн-казино Интернет-зависимость - навязчивое стремление использовать Интернет и избыточное пользование им, проведение большого количества времени в сети.

Существует несколько видов интернет зависимостей: – серфинг – бесцельное листание страниц, переходы по разным ссылкам и чтение не нужной информации;

– игровая зависимость – постоянное зависание в сетевых играх;

– финансовая зависимость – присутствует постоянное желание что-то купить в интернет-магазине;

– азартность – частое участие в аукционах, лотереях, розыгрышах, азартных интернет играх;

– зависимость от общения – отличается большим количеством переписок, участие в чатах, форумах, слишком большое количество друзей и подписчиков в социальных сетях, с которыми ребенок даже не знаком;

– киберсексуальная зависимость – частое посещение сайтов с порнографическим контентом, просмотр роликов и фотографий сексуального характера, интимные переписки;

– зависимость от видео – просмотр большого количества фильмов через интернет, сериалов, видеороликов различной тематики. Часто зритель даже не может рассказать, о чем было просмотренное видео.

В последнее время интернет-зависимость все чаще наблюдается у детей и подростков. Основным симптомом является желание в любую свободную минуту зайти в интернет. Взгляд очень долго прикован к смартфону или много времени проводится за компьютером без определенной цели. Часто пропадает реакция на раздражающие факторы вокруг, а при попытке отвлечь от данного занятия проявляется агрессия или истерика.

Признаки интернет-зависимости у ребенка:

– ребенок проводит в глобальной сети больше свободного времени, чем прежде. Его тяжело оторвать от этого занятия;

– если забрать гаджет, он не знает, чем себя занять, у него резко ухудшается настроение и наблюдается упадок сил;

– у ребенка нарушается сон, он беспокойно спит ночью;

– у школьника снижается успеваемость в учёбе, он становится рассеянным и невнимательным;

– ребенок все время проводит в интернете, даже во время обеда или ужина;

– родные люди и друзья не радуют ребенка. Виртуальное общение вытесняет реальное. Ребенок не общается со сверстниками, не играет с друзьями, пропускает школу и секции, не ходит гулять. Он предпочитает проводить время у компьютера;

– перестает выполнять свои прямые обязанности по дому: не хочет выносить мусор, мыть посуду, убирать свои вещи в шкаф;

– наблюдаются нарушения режима дня, отсутствие аппетита;

– нестабильное настроение ребенка, частая смена настроения, скрытность;

– необходимость быть «онлайн» ежеминутно. Стремление регулярно проверять социальные сети и онлайн-игры;

– если ребенок остается без интернета, он становится агрессивным и его всё раздражает, может устроить истерику.

Признаки интернет-зависимости у подростков:

– во время нахождения в сети подросток чувствует радость, как только он оказывается в обстановке без Интернета – становится раздражительным и теряет интерес к окружению;

– редко выходит на улицу, все свободное время проводит дома в сети;

– подросток перестает общаться со своими сверстниками, предпочитает виртуальное общение;

– подросток ведет пассивный образ жизни, снижается двигательная активность;

– в школе появляются проблемы с успеваемостью, плохо выполняются домашние задания;

– все разговоры и мысли только о сайтах, которые он посещает;

– не посвящает родителей в свои интересы, может им врать, стремится получить желаемое любыми способами;

– ухудшается память и внимание, снижается здоровье (ухудшается зрение, появляются проблемы с позвоночником и желудком), перестает следить за собой, становится неряшливым;

– не реагирует на просьбы;

– подросток может красть деньги и ценные вещи из дома, могут появиться денежные долги;

– снижается самооценка, перестает верить в себя.

В рамках занятий по интернет-безопасности целью педагога (и родителей) при профилактике интернет-зависимости и компьютерной зависимости детей и подростков является повышение интереса к различным сферам современного досуга. Для достижения этой цели возможны следующие задачи:

– подготовка сознания ребенка к противодействию негативных воздействий компьютерных игр;

– помощь детям в осознании их образовательных потребностей и способах их удовлетворения с помощью компьютера (развлечение, снятие стресса, познание и др.);

– информированность школьников о воспитательных возможностях школы и внешкольных учреждений (секций, кружков);

– проведение внешкольных мероприятий (дискуссий, классных часов, игр) среди обучающихся на темы, связанные с компьютерной и интернет зависимостью (например, «Место компьютера и телевидения в моей жизни»).

6. Доступность материалов, предназначенных для старшей аудитории

Пожалуй, наиболее популярны у школьников и молодежи в настоящее время экранные медиа – телевидение, кинематограф, видео, в том числе транслируемые через интернет и компьютерный монитор. Именно с экрана начинается знакомство ребенка с медиамиром. Начиная с раннего возраста, дети неплохо запоминают увиденное на экране, становятся активными телезрителями (со своими предпочтениями и любимыми героями), а к поступлению в школу, как правило, уже осваивают азы компьютерной грамотности. Особый эффект оказывает на молодежь столкновение с любым видом информационной продукции порнографического характера. Эти материалы не только стимулируют и меняют подростковое представление о сексуальных практиках, но и оказывают извращенное «образовательное» действие, служат в качестве модели и руководства к действию.

В настоящее время информационная безопасность детей при просмотре теле-, кино-,видеофильмов и программ регулируется также комплексом установленных законодательством РФ требований к содержанию аудиовизуальной информационной продукции, предназначенной для распространения среди разных возрастных групп несовершеннолетних.

Телевизионные передачи и фильмы, не предназначенные для детского просмотра, маркируются специальными значками, равноценными по величине логотипам каналов:

– для детей, не достигших возраста шести лет, - в виде цифры «0» и знака «плюс» (0+);

– для детей, достигших возраста шести лет, - в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 6 лет»;

– для детей, достигших возраста двенадцати лет, - в виде цифры «12» и знака «плюс» и (или) текстового предупреждения виде словосочетания «для детей старше 12 лет»;

– для детей, достигших возраста шестнадцати лет, - в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 16 лет»;

– для детей, - в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей».

Значок должен оставаться на экране минимум 8 секунд с момента начала передачи. Заменить его на текстовое или голосовое предупреждение телеканалы не могут.

7. Фишинг – получение доступа к логинам, паролям, банковским данным.

Цель данного вида мошенничества - получение ценных данных пользователей, которые могут быть проданы или использованы злоумышленниками для вредоносных целей, таких как вымогательство, похищение денег или кража личных данных.

Мошенники организуют рассылку сообщений по электронной почте якобы от имени банка со ссылками на поддельные страницы официальных сайтов. Вводя свои персональные данные (номера банковских карт, логины, пароли), жертва неосознанно передает конфиденциальную информацию мошенникам. А те, в свою очередь, используют сведения для завладения денежными средствами.

Аналогичные атаки осуществляются также через телефонные звонки (вишинг) и SMSсообщения (смишинг).

Подсказки, которые помогут выявить фишинговое сообщение:

– общие или неофициальные приветствия - письма без персонализации (например, «Уважаемый клиент») и формальностей, должны вызвать подозрения;

– запрос личной информации – часто используется киберпреступниками, тогда как банки, финансовые учреждения и большинство онлайн-сервисов такие запросы направляют крайне редко;

– грамматические ошибки – орфографические ошибки и опечатки, а также необычные фразы часто могут означать опасность (но отсутствие ошибок не является доказательством легитимности);

– неожиданные сообщения – любой незапланированный контакт с банком должен вызывать подозрения;

– срочность – фишинговые сообщения часто побуждают к быстрым и менее продуманным действиям;

– предложение, от которого трудно отказаться – если содержание письма слишком хорошее, чтобы быть правдой, оно, вероятно, является фишинговым;

– подозрительный домен – будет ли американский или немецкий банк отправлять письмо с китайского домена.

Отдельным подвидом необходимо рассматривать мобильное мошенничество, которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

– ссылки на фишинговые или зараженные ресурсы;

– информацию о выигрышах, которых не существует;

– ложные просьбы о помощи;

– о переводе денег на сотовый, прямые просьбы о переводе денег;

– SMS из несуществующего банка;

– просьбы перезвонить на платный номер;

– требования выкупа;

–просьбы отправить СМС, которые активируют платные услуги и другую информацию.

Для предупреждения обучающихся о фишинг-мошенничестве можно:

– рассказать о специализированных интернет-ресурсах проверки сайтов на факты совершения мошеннических действий (например, https://довериевсети.рф/, https://trustorg.com) и других сервисах контроля репутации сайта на предмет мошеннических действий;

– напомнить, что достоверный сайт обязательно содержит сведения об авторах и их контактные данные;

– обратить внимание на то, что нельзя вводить данные банковских карт на сомнительных сайтах интернет- магазинов (cvc/cvv-код, срок действия, номер карты);

– напомнить, что никому не стоит передавать или выкладывать в Сеть конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные,

адрес прописки и фактического места жительства, слишком личные фотографии.

8. Нежелательные покупки, поддельные интернет-магазины.

В интернете существует большое количество поддельных магазинов, недобросовестных продавцов и лжепредпринимателей, которые могут обмануть, не предоставить товар или завладеть персональными данными для мошеннических действий.

Покупать товар в сомнительном интернет-магазине довольно рискованно: в отличие от невиртуального магазина можно «потерять» карту, а не просто разовый платеж - если данные карты попадут в руки недобросовестных людей, они смогут присвоить всю сумму, которая находится на счету.

Основные типы афер с поддельными веб-сайтами:

– typosquatting - включает создание ложных, мошеннических или вредоносных вебсайтов с веб-адресами, очень похожими на популярные сайты, в надежде, что пользователи будут переходить на них, набирая их случайно. Рекомендуется добавить часто используемые сайты в закладки, а не вводить их вручную в адресной строке;

– мышеловка - о метод, используемый интернет-маркетологами для «ловушки» пользователей на вредоносном сайте. Интернет-магазин может отключить вашу кнопку «назад» или засыпать вас несколькими всплывающими окнами. Через некоторое время вы сможете уйти, но в некоторых случаях у вас может не быть другого выбора, кроме как перезагрузить компьютер. Меры безопасности для защиты от "мышеловки" – отключить javascript в браузере или использовать надстройку для блокировки сценариев (NoScript - позволяет пользователям выбирать, какие сценарии запускать на каждой странице);

– pagejacking - происходит, когда поисковая система направляет пользователей на ложную копию популярного веб-сайта. Оказавшись там, пользователи обычно попадают на новые страницы, содержащие рекламу и предложения. В некоторых случаях эти сайты могут быть злыми или содержать непристойные материалы, такие как содержание ненависти или порнографию. Доступ к сайтам через "Избранное" или "Закладки" может помочь избежать неприятных последствий;

– фарминг - перенаправляет пользователей с законных сайтов на мошеннические магазины, которые отслеживаю вводимую информацию, такую как номера кредитных карт, банковские данные, а также имена пользователей или пароли. Для этого рассылают вирус, который заставляет компьютеры связывать законное доменное имя с мошенническим вебсайтом или атакуют сервер веб-сайта, так что каждый посетитель попадает на вредоносную версию сайта. Чтобы не стать жертвой фарминга, необходимо убедится, что вы посещаете защищенные веб-сайты (адрес веб-сайта должен начинаться с префикса https://). Также для предупреждения о недействительности сертификата веб-сайта (запись подлинности) следует установит программное обеспечение для обеспечения безопасности в Интернете (Kaspersky, McAffee или AVG).

Особенно рекомендуется обратить внимание и избегать сайты и сервисы:

– продающие технику, на которой отсутствует русификация. Это является одним из ризнаков контрабандного товара либо оборудование уже на заводе не планировалось поставлять в Россию;

– использующие для приема платежей электронные кошельки, поскольку такие сервисы предоставляют возможность принимать платежи сразу после регистрации, указав только электронную почту. E-mail нельзя отследить, что сказывается на отсутствие возможности установить личность продавца;

– которые не имеют пунктов самовывоза или своих офисов.

Для предупреждения обучающихся о мошенничестве при заказе через Интернет можно объяснить некоторые правила:

– обязательно нужно проверить интернет-магазин перед совершением покупки: на официальном сайте должны быть приведены сведения о правоустанавливающих документах (свидетельство о регистрации в налоговом органе, код ОКВЭД, ИНН, ОГРН), соглашение на использование и обработку персональных данных, адрес фактического расположения, данные о потребительских свойствах товара;

– следует доверять только известным и фирменным магазинам - в известных интернет-магазинах типа Wildberries, OZON и других есть все необходимое. С их помощью данные карты будут максимально защищены, потому что у крупных компаний отлаженная и безопасная система обработки;

– следует обращать внимание на адрес при входе на сайт обращать внимание на адрес - убедитесь, что вы действительно находитесь на amazon.com, а не на anazon.com или что в адресе после названия известного магазина нет какого либо окончания (например, «известный_магазин.ru-acw.xyz). Также нужно иметь ввиду, что доменные имена мошеннических магазинов, как правило, длинные и сложные, но в них присутствует имя известного бренда;

– не сообщать свои персональные данные (в том числе пароль от интернет-банкинга) и не переводить денежные средства лицам, которые не являются сторонами сайта;

– следует периодически проверять карту - если ее данные попадут в чужие руки, велика вероятность, что деньги «проскользнут» незамеченными - при небольшой сумме покупке или приобретении подарочных карт банк не заподозрит, что транзакция неавторизована, а вы будете частично ограблены;

– следует использовать только свой компьютер, планшет или телефон, к которым мало кто имеет доступ, при входе в интернет-банк или при совершении покупок в Интернете.

Если все-таки нужен интернет-банкинг с чужого компьютера, не забывать удалить свои данные и не оставлять информацию, с которой вошли в систему - лучше всего открыть режим инкогнито или приватный режим браузера, после закрытия которого все данные и история страниц будут автоматически удалены. Чтобы безопасно выйти из интернетбанкинга по окончании работы обязательно воспользоваться кнопкой «Выйти»;

– следует избегать нереалистичных предложений – если сайт предлагает нереальные цены на новые модели мобильных телефонов или на новейшую дизайнерскую одежду – это мошенник. Конечно, часто будут встречаться скидки, но в этом случае необходимо наблюдать, на каком сайте вы находитесь, что мотивирует эту скидку и т. д.

9. Информация о легком заработке.

Сейчас в сети Интернет набирают популярность объявления о легком и высоком заработке для подростков. Зачастую такая работа связана с вовлечением ребят в мошеннические или преступные схемы. Как правило, речь идет о распространении наркотических средств: подростки делают «закладки» в назначенных куратором местах, а затем их забирают клиенты. Стоимость такой подработки для школьников весьма привлекательна. Нередко подростки соглашаются, не догадываясь о характере доставляемого товара, однако иногда желание заработать перевешивает здравый смысл, и согласие участвовать в распространении наркотиков дается сознательно с расчетом остаться безнаказанными.

В рамках мероприятий по информационной безопасности обучающимся можно рекомендовать:

– анализировать любые «привлекательные» объявления на адекватность;

– всегда проверять информацию о работодателе, а проверив - настаивать на оформлении официальных трудовых отношений (с 14 лет) или договора гражданскоправового характера (с 15 лет) - если речь не идет ни о чем незаконном, работодатель должен согласиться;

– выяснять содержание и условия подработки до мелочей (почему так оценивается, что конкретно нужно делать, что нужно везти, какой товар доставлять);

– если что-то смущает – не стесняться спрашивать и выяснять любые подробности;

– всегда помнить, что за легкую работу ни один работодатель не будет расплачиваться крупной суммой денег;

– обращать внимание на предложения сделать что-то анонимно. Это один из маркеров того, что вас вовлекают в мошенническую схему.

10. Съемка фото и видео для размещения в сети Интернет, сопряженная с опасностью для жизни и здоровья

В последнее время среди интернет-пользователей набирает популярность фото- и видеосъемка как повседневных, так и ярких жизненных моментов, и размещение данного контента в сети Интернет. Некоторые примеры такого поведения детей:

– подросток становится невольным свидетелем вооруженного конфликта, стрельбы, взрыва и первым делом снимает происходящее на мобильный телефон. Вместо того чтобы предпринять необходимые меры безопасности (убежать, вызвать полицию), он снимает «уникальное видео» ради популярности в Сети, рискуя жизнью и здоровьем;

– выбор подростком опасных или экстремальных увлечений. Например, «руфинг» (прогулки по крышам), «скайуокинг» (покорение самых высоких точек в городе без специального снаряжения) или «зацепинг» (проезд вне салона электропоезда, трамвая – на крыше или подножке). Ради популярности в Интернете дети стремятся заснять свои «подвиги», что ведет к негативным последствиям. Такие увлечения сами по себе представляют смертельную опасность, а использование камеры только увеличивает риск оступиться, потерять равновесие или не заметить угрозу;

– стремление поразить интернет-друзей яркими или опасными фотографиями, сделанными в формате селфи. Как в России, так и в мире зафиксирована масса смертельных исходов при попытке сделать собственную фотографию в опасных местах, которые уже получили название «селфиубийства». Селфи на воде, на краях обрывов или скал, на железных и автомобильных дорогах, на крышах домов или промышленных объектов, вблизи линий электропередач могут привести к крайне негативным последствиям для жизни и здоровья ребенка.

Предотвратить подобные ситуации можно через формирование у обучающихся культуры личной безопасности. Она состоит в готовности защитить себя и окружающих от неблагоприятного воздействия, угроз и наступления нежелательных последствий. В рамках мероприятий по информационной безопасности обучающимся можно объяснить:

– объяснить, что при возникновении опасных ситуаций необходимо в первую очередь, позаботиться о безопасности себя и других людей, а затем вызвать полицию;

– провести беседу на тему опасных увлечений, при этом услышать от обучающегося аргументы в пользу его хобби. Главное — занять доброжелательную позицию со своей стороны, ненавязчиво предложить альтернативные виды деятельности, проходящие в безопасных условиях.

Важно не переусердствовать, но при этом донести до ребенка посыл, что он не безразличен вам, своей семье, близким и друзьям

5. Антитеррористическая безопасность. Действия персонала школы и обучающихся при различных видах угроз.

По пятому вопросу выступил Тарзиманов Ш.А., преподаватель-организатор ОБЗР

Педагогический коллектив школы был ознакомлен с памяткой «Алгоритмы действий персонала образовательной организации, работников частных охранных организаций и обучающихся при совершении (угрозе совершения) преступления в формах

вооруженного нападения , размещения взрывного устройства, захвата заложников, срабатывания на территории образовательной организации взрывного устройства, в том числе доставленного беспилотным аппаратом, нападения с использованием горючих жидкостей , а также информационного взаимодействия образовательных организаций с территориальными органами МВД, Росгвардии и ФСБ России»

Решение:

1. Определить приоритетным направлением работы на новый учебный год поддержание безопасной, комфортной психолого-педагогической образовательной среды.
2. Усилить работу по ранней профилактике деструктивного поведения учащихся и оказанию психолого-педагогической помощи участникам образовательных отношений.
3. Ввести новые цифровые ресурсы: государственная информационная система «Профилактика» и сервис «Цифровой психолог» во ФГИС «Моя школа».
4. Продолжить межведомственное взаимодействие по вопросам профилактики деструктивного поведения обучающихся.
5. Усилить работу с родителями (законными представителями) обучающихся по повышению родительской компетентности, профилактике семейных конфликтов и формированию ответственного поведения несовершеннолетних.
6. Педагогическому коллективу регулярно повышать квалификацию по вопросам профилактики деструктивного поведения обучающихся и взаимодействию с семьей.
7. Педагогическому коллективу изучить памятку «Алгоритмы действий персонала образовательной организации, работников частных охранных организаций и обучающихся при совершении (угрозе совершения) преступления в формах вооруженного нападения , размещения взрывного устройства, захвата заложников, срабатывания на территории образовательной организации взрывного устройства, в том числе доставленного беспилотным аппаратом, нападения с использованием горючих жидкостей , а также информационного взаимодействия образовательных организаций с территориальными органами МВД, Росгвардии и ФСБ России»

Директор школы С.В. Халманова

Секретарь Е.Г. Плешакова