**Запрещенный контент на онлайн - уроках**

Практически каждый из нас является счастливым обладателем мобильного телефона, а многие – и компьютера.

Дети, подростки, молодежь хотят знать информации намного больше, чем им могут предоставить родители, школа и общедоступные Интернет –ресурсы. И их любопытство порой оказывается на грани, а иногда и за гранью дозволенного.

С 1 сентября 2012 года в РФ действует Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Руководство школы, учителя несут обязанность защищать психическое здоровье, моральное и нравственное развитие детей. На компьютерах, предназначенных для обучения детей, должна быть установлена специальная система блокирования доступа к информации в интернете, например, к интернет-площадкам с порнографическим и националистическим контентом, информацией о наркотиках и призывами к осуществлению террористической деятельности.

Аналогичные требования существуют и при реализации общеобразовательных программ с применением дистанционных технологий.

Из этого следует правомерность привлечения к административной ответственности по части 2 статьи 5.57 КоАП (нарушение права на образование и предусмотренных законодательством об образовании прав и свобод обучающихся образовательных организаций) руководства школы за появление порноконтента в эфире онлайн-урока.

Однако необходимо учитывать развитие компьютерных технологий, чрезвычайность ситуации, неподготовленность школ к дистанционному обучению в условиях пандемии, отсутствие должной оснащенности учителей программными ресурсами, которые позволили бы исключить подобные ситуации.

Учителя вынуждены сами находить способы обучения и платформы, на которых можно проводить уроки онлайн. При этом педагогический персонал зачастую не обладает специальными знаниями в области компьютерных технологий.

Бывают такие случаи, что вовремя онлайн –урока дети могут включить запрещенное видео (порнографического характера). Которое влечет за собой психологическую травму у некоторых детей.

То есть школа, с одной стороны, несет ответственность за предоставляемые образовательные услуги, с другой — оказывается пострадавшим, поскольку в результате действий распространителя причиняется вред деловой репутации образовательного учреждения, к школе может быть предъявлен иск от родителей.

Если ребенку причинен моральный вред (психологическая травма), у родителей появляется право на обращение в суд. Ответчиком, на мой взгляд, становится и лицо, распространившее порноконтент, и школа. В этом случае родителю в ходе судебного разбирательства следует доказать факт демонстрации порноконтента во время онлайн-урока, а также обосновать причинение морального вреда ребенку — например, представить справку от психолога.

Уголовную ответственность, предусмотренную статьями 242, 242.1 УК РФ, может понести лицо, достигшее шестнадцатилетнего возраста, которое выложило порноролик в эфир, тем самым публично распространив порноконтент. Если таким лицом был кто-то из школьников, если в судебном порядке будет установлено, что его действиями причинен моральный либо материальный вред, то взыскан он будет либо с него самого, либо (если ребенку еще нет 16) с родителей.

Проблема с атаками на школьные онлайн-уроки существует, разумеется, не только в России. На карантине или самоизоляции сейчас находится плюс-минус весь мир, дети массово учатся онлайн, а хакеры и пранкеры этим пользуются. В англоязычном (а теперь уже и в международном) сообществе появилось даже новое понятие «зумбомбинг» — по названию сервиса Zoom, с помощью которого в большинстве случаев и происходит коммуникация. Новое слово используется, когда речь идет о хакерском вторжении во время учебной, рабочей или личной онлайн-конференции.

Zoom — приложение, с помощью которого можно организовывать видеоконференции с неограниченным количеством участников, возможностью писать в чат и другими удобными опциями — за время пандемии стало самым скачиваемым в App Store, обогнав таких монстров, как WhatsApp, Google и TikTok. Но ни учителя, ни сам сервис оказались не готовы к новой реальности. Первые не до конца разобрались с техникой безопасности в сети, вторые не успели доработать приложение, чтобы не допустить хакерских атак.

Чтобы использование приложения в процессе обучения было максимально эффективным и безопасным, стоит соблюдать несколько ключевых правил:

1. Защищайте каждую конференцию паролем и не делитесь ссылками на нее в социальных сетях. Нужно понимать, как происходит процесс подключения к конференциям. Если онлайн-встреча не защищена паролем, то к ней могут подключиться сторонние люди. Важно не только устанавливать пароль на конференцию, но и передавать его безопасным образом другим участникам (например, не выкладывать в открытый доступ в соцсетях).

2. Включите «комнату ожидания». Идея этой функции в том, что желающие присоединиться к конференции попадают в «лист ожидания» и остаются в нем, пока организатор онлайн-встречи не одобрит их участие. Эта функция может быть особенно полезна, если вы подозреваете, что пароль от конференции все же попал в открытый доступ.

3. Защитите свою учетную запись в Zoom (и в любом другом сервисе). Для этого следует использовать надежный пароль (от 12 символов с буквами в разном регистре, цифрами и спецсимволами) и создать уникальные пароли для всех учетных записей. Кстати, в тех сервисах, где это возможно, нелишним будет настроить двухфакторную аутентификацию для входа в аккаунт.

4. Скачивайте приложение только с официального сайта, а приложения для мобильных устройств — в App Store или Google Play. Как выяснили наши эксперты, в марте 2020 года число вредоносных файлов, названия которых содержат отсылки к популярным сервисам для онлайн-конференций (WebEx, GoToMeeting, Zoom и т. д.), увеличилось почти втрое по сравнению с прошлым годом. Это значит, что злоумышленники пытаются замаскировать вредоносные программы под клиенты для видеосвязи.

5. Изучите настройки демонстрации экрана. Zoom, как и многие другие приложения для видеоконференций, позволяет показывать другим участникам онлайн-встречи экран подключенного устройства. Перед уроком проверьте следующие настройки: кто может демонстрировать экран (только организатор или любой участник конференции) и разрешена ли одновременная демонстрация экранов нескольких участников. Эти опции лучше отключить, если по программе урока презентацию будет показывать только учитель.

6. Предложите ученикам в ходе конференции использовать только реальные имена, чтобы было понятно, кому ставить отметку за урок. К тому же это поможет снизить количество анонимных высказываний не по теме занятия.

Приложений для видеоконференций сегодня существует огромное количество, но найти одно универсальное, которое бы подошло абсолютно для всех форматов занятий, достаточно сложно. И все же, когда в школе сформированы единые требования к онлайн-платформе (иными словами, все учителя и ученики работают в одних и тех же сервисах), обучение проходит в более комфортных условиях.

Альтернативой тому же Zoom могут стать Microsoft Teams, Google Meet, Discord — аналогичные, простые в использовании сервисы со своими преимуществами. Однако и при их использовании стоит изучить технику безопасности и не забывать основные правила организации сетевых конференций.