О НЕКОТОРЫХ СПОСОБАХ ПРЕДОТВРАЩЕНИЯ СРЫВА ВИДЕОКОНФЕРЕНЦИИ В ZOOM

Полищук Наталья Алексеевна
старший преподаватель
ГОУ ВО ЛНР «Луганский государственный педагогический университет», г. Луганск, ЛНР
e-mail: nata_pl@list.ru
Полищук Руслан Васильевич
ГУ «Луганский республиканский центр дополнительного профессионального образования», г. Луганск, ЛНР
e-mail: polan.lg.ua@rambler.ru

Пандемия внесла свои коррективы во все сферы жизни человечества, не стала исключением и система образования. Учебные заведения были вынуждены перейти на новую для многих дистанционную форму обучения. Многим школам, университетам и учебным центрам пришлось искать готовое программное обеспечение для организации видеосвязи, позволяющее проводить занятия в онлайн-режиме. Особую популярность в мире и в России, в частности, получила программа для организации видеоконференций – Zoom. Безусловно эта программа обладает рядом преимуществ перед другими, но в данной работе остановимся на следующей существенной проблеме, с которой пришлось столкнуться многим преподавателям, так называемом зумбомбинге.

Зумбомбинг – это одна из разновидностей кибератак, заключающейся в том, что к видеоконференции присоединяется сторонний пользователь, с целью сорвать ее проведение. Зачастую такие пользователи пишут на экране оскорбительные надписи, демонстрируют фотографии, транслируют аудио и видеоролики непристойного характера, то есть всячески мешают проведению занятий.

Кто же скрывается за маской «зумбомберов»? Зачастую это молодые люди, которые таким образом самоутверждаются, они снимают видео о своих сомнительных достижениях и выкладывают их в сеть. Данные для подключения к видеоконференции они находят несколькими способами: берут их из открытого доступа из объявлений о запланированных конференциях, размещенных в сети; пишут и используют для взлома специальные программы, генерирующие идентификаторы конференции и подбирающие пароли; получают данные для участия в конференции от заказчика.

Кто выступает в роли заказчика? Как это ни странно звучит, но заказчиками выступают сами обучающиеся. Причинами такого поведения может послужить желание развлечься, оскорбить или унизить кого-то из участников конференции, сорвать занятие из-за собственной неподготовленности к нему.

В сети интернет созданы целые темы на форумах, группы в Telegram, Viber, WhatsApp и VK, в которых желающие размещают ссылку на конференцию с информацией о времени начала, имени преподавателя и нескольких настоящих именах и фамилиях учеников. Примеры таких групп в Telegram можно увидеть на рисунке (рис. 1).

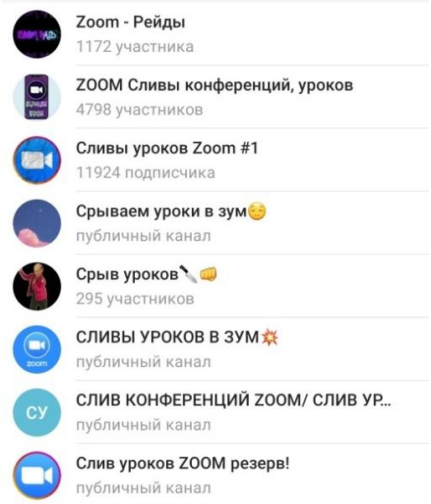

Рисунок 1 – Группы зумбомбинга в Telegram

В этих же группах, а также на специализированных каналах YouTube обсуждают результаты зум-рейдов, публикуют видео, скриншоты возмущенных и удивленных лиц участников конференций.

Таким образом, зумбомбинг – серьезная проблема дистанционного образования. Надоедливые интернет-тролли вторгаются в чужие видеоконференции, пытаясь их сорвать. Однако есть несколько способов, позволяющих обезопасить проведение онлайн-уроков. В данной работе приведены некоторые из них.

Многие учащиеся в самом начале дистанционного обучения воспринимали интернет не как средство обучения, а как средство развлечения и отдыха. Поэтому очень важно было выработать и донести до них правила поведения при проведении онлайн-занятий. Некоторые школы в настоящее время уже опубликовали на своих сайтах правила поведения, в которых закрепили нормы поведения, запреты и ответственность учащихся.

Рассмотрим теперь техническую сторону вопроса. В первую волну пандемии преподаватели были вынуждены экстренно переходить на онлайн-обучение, зачастую плохо владея или не владея совсем навыками работы с программой Zoom. Они создавали запланированные видеоконференции, для входа в которые не требовался пароль, либо выкладывали идентификатор и пароль конференции на сайте школы в открытый доступ. Это позволяло сторонним пользователям сети интернет беспрепятственно присоединяться к занятию и срывать его.

Накопленный за период дистанционного обучения опыт позволил сформировать некоторые принципы организации онлайн-уроков в программе Zoom.

1. Каждый обучающийся должен быть зарегистрированным пользователем в Zoom, кроме того при регистрации необходимо указывать свои настоящие фамилию и имя. Вряд ли кто-то из учеников захочет в открытую срывать занятия, боясь последующего наказания. Кроме того, это позволит преподавателю контролировать посещаемость занятия и будет способствовать дисциплине и ответственности учащихся. Пользователей без имени или не из списка учащихся преподаватель может сразу заблокировать. Для этого достаточно перейти к списку участников, навести курсор на имя пользователя и выбрать «Удалить».

2. Целесообразно при планировании конференции создать «Зал ожидания». Это автоматически запретит вход в конференцию без организатора или раньше него. Преподаватель сможет подключать участников по одному или собрать всех в зале ожидания и затем подключить сразу всех. Наличие «Зала ожидания» в конференции даёт возможность перед допуском участников к конференции идентифицировать их и удалить нежелательных гостей.

3. Одной из мер по предотвращению зумбомбинга может стать обязательное требование к участникам онлайн-занятия – наличие у них включенной веб-камеры. Это позволит гарантированно идентифицировать личность участника. Однако не у всех пользователей скорость интернет-соединения позволяет выполнять это требование во время всего занятия. В этом случае после идентификации пользователя можно разрешить учащемуся отключить камеру, и включать её только при необходимости.

4. После того, как все учащиеся подключились, организатор, перейдя в настройки безопасности и поставив галочку напротив соответствующего пункта (рис. 2), сможет блокировать конференцию. Это даст возможность сделать встречу закрытой и новые участники не смогут присоединиться к ней.

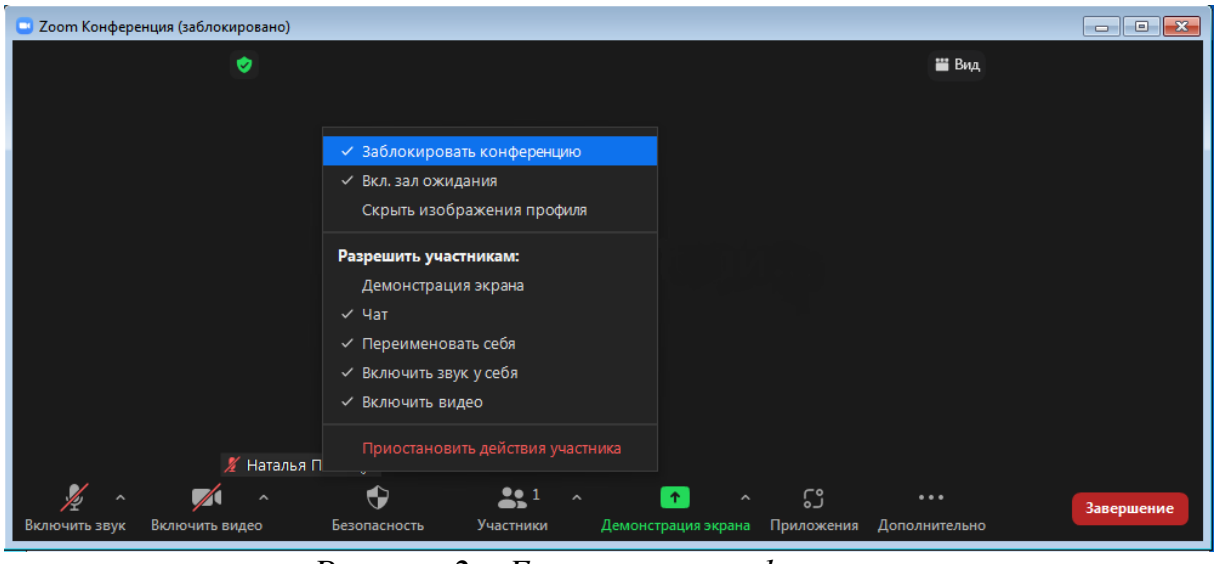

Рисунок 2 – Блокировка конференции

5. Чтобы избежать появления на экране не запланированных организатором рисунков, картинок или видео, необходимо в настройках управления организатора конференции отключить совместный доступ к экрану (рис. 3).

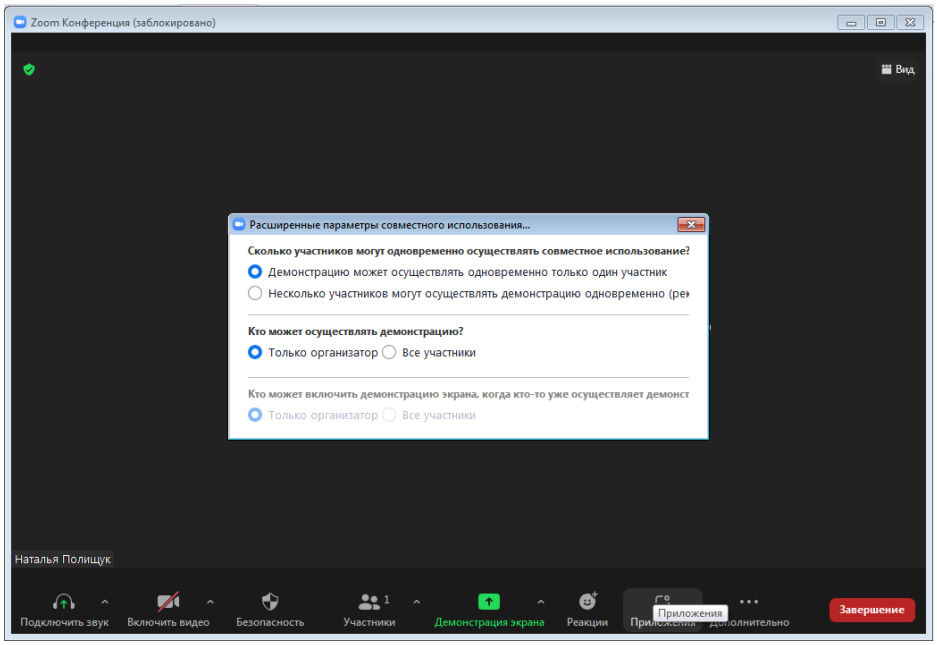

Рисунок 3 – Настройка демонстрации экрана

6. Отключить в настройках возможность обмениваться сообщениями (рис. 4). Это не даст участникам возможности отвлекать друг друга перепиской, так же как и на обычном уроке переговариваться. В случае необходимости, можно разрешить возможность обмениваться сообщениями организатору и соорганизаторам.

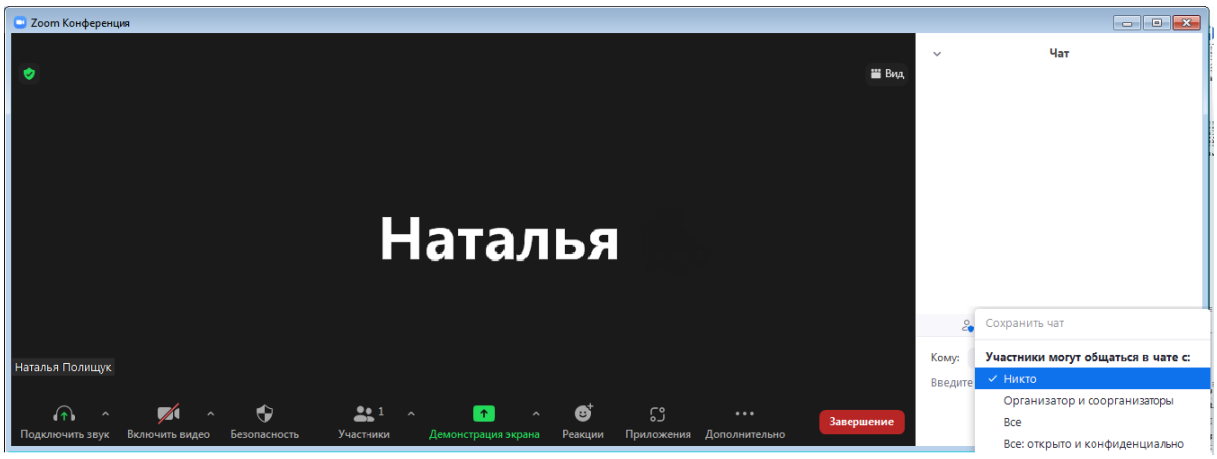

Рисунок 4 – Настройка чата

7. Во время демонстрации экрана отключить участникам конференции возможность комментирования (рис. 5). Это не позволит учащимся несанкционированно рисовать или писать на общем экране.

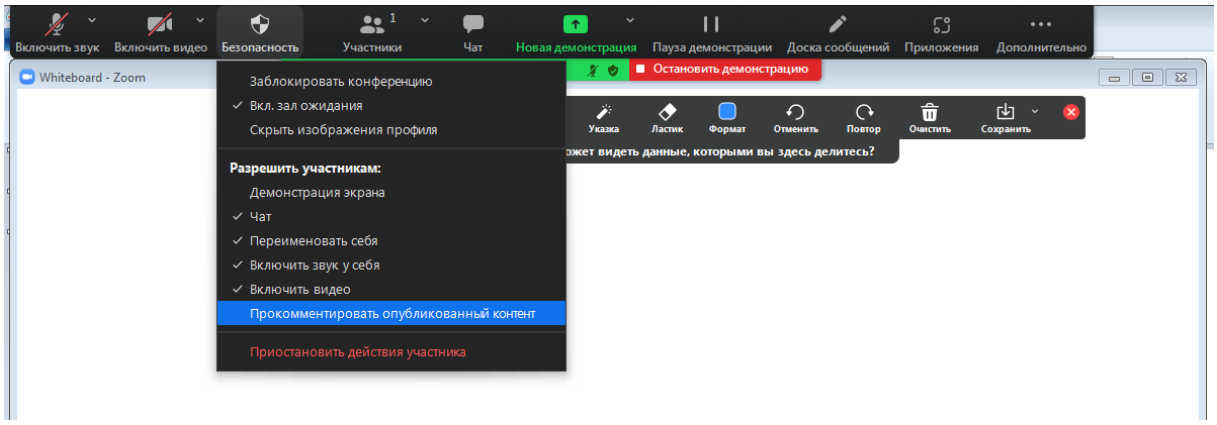

Рисунок 5 – Отключение возможности комментирования во время демонстрации экрана

Следует отметить, что преподавателю перед планированием и проведением видеоконференций в Zoom обязательно необходимо внимательно изучить инструкции, представленные на сайте разработчика в разделе «Безопасность и конфиденциальность». А также, кроме технической стороны вопроса, продолжать проводить разъяснительную и воспитательную работу с учениками и их родителями. Ученикам необходимо сообщить о том, что их действия, направленные на срыв онлайн-уроков, могут классифицироваться как хулиганство и за свои действия они могут понести административную ответственность.

Все эти меры в комплексе помогут решить рассмотренную проблему.

Литература

1. Ефимова А. «Класс был в шоке» : чем грозит срыв школьных онлайн-занятий [Электронный ресурс] / А. Ефимова // Газета.ру : российское интернет-издание. – URL: https://www.gazeta.ru/social/2020/04/22/13057963.Shtml. – Заглавие с экрана. – Дата обращения 15.12.2021.
2. Zoom [Электронный ресурс] : Официальный сайт компании Zoom. – URL: https://zoom.us/. – Заглавие с экрана. – Дата обращения 15.12.2021.