

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по онлайн-безопасности и защите
учащихся во время дистанционного образовательного процесса в начальном,
гимназическом и лицейском образовании на 2020-2021 учебный год**

Введение

Онлайн-безопасность учащихся должна быть одним из приоритетов дидактического персонала в контексте дистанционного образовательного процесса. Учитывая специфические особенности образовательного процесса в контексте эпидемиологического кризиса COVID-19, при реализации любой модели, выбранной на уровне учебного заведения для организации образовательного процесса в 2020-2021 учебном году, задача содействия онлайн-безопасности учеников будет обеспечиваться посредством:

- Формирования навыков и умений ответственного и безопасного поведения в виртуальной среде;
- Предоставление информации, средств и инструментов для оповещения о случаях насилия в онлайн среде со стороны сверстников и взрослых;
- Обеспечения доступа учащихся к веб-платформам и инструментам, используемых в дистанционном образовательном процессе.

Методические рекомендации по онлайн-безопасности учащихся при дистанционном образовательном процессе были разработаны на основании:

- Кодекса об образовании РМ № 152/2014, ст. 135 п. h), k), l);
- Учебного плана для начального, гимназического и лицейского образования на 2020-2021 учебный год;
- Действующего Куррикулума по школьным предметам для начального, гимназического и лицейского образования;
- Методических рекомендаций по организации 2020-2021 учебного года в эпидемиологическом контексте COVID-19, для учебных заведений начального, гимназического, лицейского и внешкольного образования, утвержденных приказом МОКИ № 840 от 13.08.2020 г.;
- Методологии продолжения дистанционного образовательного процесса в условиях карантина для учебных заведений начального, гимназического и лицейского образования, утвержденной приказом МОКИ № 351 из 19.03.2020 г.;
- Стандартов минимального оснащения кабинетов по школьным предметам в общеобразовательных учреждениях, утвержденных Приказом № 193 от 26.02.2019 года;
- Инструкций по обработке персональных данных в сфере образования, утвержденных приказом Национального центра по защите персональных данных Республики Молдова № 03 от 21 января 2015 года.

Методические рекомендации определяют способ участия дидактического и руководящего персонала в обеспечении безопасности и защиты учащихся в дистанционном образовательном процессе, включая online.

Основные понятия

Онлайн-безопасность учащихся – это результат ряда мер, принятых для защиты благополучия ребенка в виртуальной среде от возможных рисков, которые могут повлиять на его физическую и эмоциональную целостность.

Онлайн-насилие – использование компьютерных систем для провокации, содействия или угрозы применения насилия в отношении лиц, которое причиняет или может причинить физический, сексуальный, психологический или экономический вред или страдания, и может включать использование обстоятельств, характеристик или уязвимости этих лиц.¹

Злоупотребление уязвимости детей в Интернете – любая форма физического, эмоционального или сексуального насилия, которым подвергаются дети в виртуальной среде, или которым способствует использование информационно-коммуникационных технологий.

Онлайн-защита – результат ряда мер, принятых для обеспечения защиты данных, информации и цифровых устройств человека.

I. Формирование и развитие навыков и умений ответственного поведения в виртуальной среде

1.1. На институциональном уровне руководители доуниверситетского и среднего образования должны планировать и выполнять следующие действия:

- а) Пересмотреть годовой план деятельности учебного заведения, включив в него специальный раздел «Обеспечение защиты жизни и здоровья детей», в котором будут четко спланированы действия, направленные на продвижение онлайн-безопасности учеников в дистанционном образовательном процессе, исходя из положений п. 1.7 Учебного плана для начального, гимназического и лицейского образования на 2020-2021 учебный год, утвержденного Приказом МОКИ № 396 от 06.04.2020 г.
- б) Запланировать и провести следующие внеклассные мероприятия:

Международный День безопасности в Интернете (отмечается ежегодно во второй вторник февраля), в рамках которого будут проводиться мероприятия по информированию и повышению осведомленности о рисках в Интернете, укреплению цифровой культуры и повышению уровня осведомленности об угрозах в виртуальной среде, а также о способах защиты в Интернете для учеников, преподавателей и родителей.

Ежемесячник по кибербезопасности (отмечается ежегодно в октябре), в рамках которого будут проводиться информационные мероприятия об онлайн-рисках и способах защиты в Интернете, для учеников, преподавателей и родителей.

1.1. Преподаватели будут обучать учащихся I-XII классов умениям и навыкам ответственного онлайн-поведения в рамках следующих дисциплин:

- *Технологическое воспитание*, куррикулумная область *Технологии*, Модуль *Цифровое воспитание*, согласно Учебному плану;

¹ Согласно определению Комитета по Конвенции о киберпреступности, Рабочей группы по киберзапугиванию и другим формам онлайн-насилия, особенно над женщинами и детьми, доступно по адресу <https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914>

- *Развитие личности*, куррикулумная область *Личностное развитие*, Модуль *Безопасность личности*, согласно Учебному плану;
- Дисциплина по выбору *Медиаобразование*, Модуль *Мультимедиа и новые медиа в жизни ребенка*, *Информированный потребитель и новые медиа* и *Виртуальная среда и ее воздействие*, согласно Учебному плану.

1.2. Кроме того, в контексте обучения учеников трансверсальным/трансдисциплинарным навыкам, развитие безопасного поведения в онлайн-среде будет осуществляться и на основе интегрированного принципа по всем школьным предметам. Преподаватели изучат возможности, предоставляемые учебной программой по таким предметам как *Информатика*, *Развитие личности*, *Гражданское воспитание*, *Румынский язык* и т.д. в целях обучения учеников умениям и навыкам, необходимым для ответственного поведения в виртуальной среде, используя дидактические материалы и разнообразие доступных образовательных технологий.

1.3. Классный руководитель будет выполнять следующие действия:

- a. В случае если он не обучает дисциплине *Развитие личности*, он не реже одного раза в месяц будет проводить с учениками мероприятие по онлайн-безопасности в соответствии с годовым учебным планом учебного заведения и в соответствии с образовательными особенностями класса, возрастом и интересами/запросами учеников, в сотрудничестве с другими учреждениями и организациями.
- b. На собраниях с родителями, в зависимости от возрастной специфики детей, обсуждается:
 - поведение детей в онлайн-среде в зависимости от возраста и связанных с ним возможных рисков;
 - важность дружеского общения родителей с детьми об: интересах в онлайн-среде, опубликованном или/и распространяемом контенте, дружбе в онлайн-среде;
 - наблюдение за поведением ребенка и возможными признаками того, что он может столкнуться с неприятной ситуацией в онлайн-среде/жестоким обращением в онлайн-среде;
 - ресурсы и информация о безопасности в Интернете, а также инструменты для получения совета и помощи в случае возникновения подозрительной ситуации или ситуации жестокого обращения с детьми в онлайн-среде.
- c. В контексте дистанционного образовательного процесса контролирует поведение учеников во время школьных и внеклассных занятий в виртуальной среде;
- d. Систематически наблюдает за поведением ребенка в Интернете, оценивает, планирует и осуществляет начальное вмешательство.

1.4. При дидактическом планировании занятий по онлайн-безопасности преподаватели будут учитывать следующие аспекты:

- Целью деятельности по безопасности в Интернете является развитие навыков критического мышления детей в онлайн-среде.
- Образовательные цели направлены на формирование онлайн-поведения, ориентированного на уважение, ответственность и оценку возможных рисков.
- Образовательные ресурсы необходимо подбирать с учетом рекомендаций специалистов, возрастных особенностей детей и целевой группы, к которой они обращаются.

- Стратегии обучения должны выбираться в соответствии с возрастными особенностями учеников, спецификой и особенностями обучения и интересов.
- Каждый педагог выберет формы оценки проводимой педагогической деятельности, ориентируясь на дальнейшее определение потребностей учеников со ссылкой на приобретение навыков для разрешения различных ситуаций в онлайн-среде.

1.5. Преподаватели, которые проводят дистанционное обучение, в том числе онлайн, используя одну или несколько веб-платформ, должны предпринимать следующие действия, чтобы предотвратить различные типы онлайн-рисков для благополучия ребенка:

- а. Проводить раз в месяц беседы с учениками об их безопасности в среде Интернет и анализировать практические примеры со ссылкой на ситуации злоупотребления уязвимости детей в Интернете, которые могут иметь место как в личной онлайн-деятельности, так и в деятельности, связанной с учебным процессом, например:
 - ✓ травля в онлайн среде со стороны знакомых сверстников или других неизвестных лиц;
 - ✓ подвержение ребенка воздействию неприемлемого или/и насильственного контента, со стороны сверстников или других неизвестных лиц;
 - ✓ шантаж и манипуляции со стороны известных или неизвестных лиц;
 - ✓ навязывание ребенку различных видов действий неприемлемого характера в онлайн-среде.

При осуществлении этих мероприятий будут приняты во внимание рекомендации Куррикулума, а также могут быть использованы дидактические сценарии, разработанные Международным Центром *La Strada* в сотрудничестве с МОКИ, доступные по адресу www.siguronline.md, в рубрике Педагоги/преподаватели, учебные ресурсы.

- б. Не распространять, без письменного согласия родителя/опекуна, в социальных сетях или на других платформах фотографии и/или видеоролики, сделанные во время урока, на которых можно идентифицировать учеников;
- с. Обсуждать с учениками необходимость защиты персональных данных в онлайн-среде и того, что связано с учебной деятельностью, организованной во время дистанционного образовательного процесса, в том числе в среде Интернет.

II. Предоставление детям информации и инструментов для оповещения о случаях онлайн-насилия со стороны сверстников и взрослых;

2.1. Преподаватели будут информировать учеников о том, что любой онлайн-контент (сообщение, комментарий, фотография, видеоролик и т.д.), принадлежащий им и распространяемый без их согласия, унижительные или оскорбительные сообщения, запугивающие действия, фейковые аккаунты, созданные с использованием их персональных данных, действия с применением шантажа, неприятные комментарии или комментарии с неприемлемым подтекстом, можно удалить, сообщив о них на платформу, где они были опубликованы. У каждой службы или платформы в Интернете есть определенные правила использования, Условия использования и процедуры сообщения об оскорбительном контенте в Интернете.

2.2 Преподаватели проинформируют учеников об альтернативных службах по информированию и консультированию онлайн в ситуациях жестокого обращения в Интернете, таких как: www.siguronline.md – онлайн служба поддержки и помощи детям которые подверглись насилию в интернете; телефон доверия для детей: 116-111, Зеленая

2.3. Ученикам рекомендуется сообщать классному руководителю о любых подозрительных случаях/ситуациях в онлайн-среде, касающихся их лично, либо их коллег.

2.4. В условиях дистанционного образовательного процесса, классный руководитель рассматривает все возможные случаи насилия в отношении ребенка в виртуальной среде и, в зависимости от выявленной ситуации, будет применять следующие стратегии вмешательства, согласно описанным ниже сценариям:

а. Преподаватель замечает или ученики сообщают ему о подключении незнакомых, неопознанных лиц к веб-платформе (Например: Человек, которого ученик не знает, подключился к учебному процессу на платформе; В чате платформы появляются комментарии от неизвестного пользователя; Ученик получил ссылку для доступа к учебной деятельности от пользователя, которого он не знает; Неизвестный пользователь запрашивает доступ к уроку, проводимому преподавателем на платформе; Учебные задания, загруженные на веб-платформу, удаляются или блокируются; В виртуальном классе идентифицируются файлы, которые, похоже, не принадлежат ученикам и т.д.)

Преподаватель:

- проверит или обратится за помощью к специалисту учебного заведения, чтобы тот проверил, если для аккаунта с которого осуществляется обучение на платформе установлены все меры безопасности для устранения проблемы;
- также обратится за помощью к другим специалистам: школьному психологу, администрации, полиции, службам по консультированию и информированию о случаях жестокого обращения с детьми, если выявлена неприятная ситуация, с которой уже столкнулся ученик.

б. Педагог является свидетелем, вместе со всем классом, жестокого обращения с одним или несколькими учениками во время преподавания на веб-платформе;

1. Он попросит учеников, используя общий или прямой чат, отключиться от урока и не подключаться по той же ссылке.

2. Педагог может попытаться определить имя пользователя, который вошел в систему и предпринял неправомерные действия в адрес учеников или/или преподавателя, может сделать скриншот, если неизвестный человек открыл экран с содержанием вредного для учеников контента.

3. В результате инцидента школьный психолог подготовит план работы с классом/учеником, с которым произошла ситуация.

4. Учебное заведение будет сотрудничать с компетентными органами или/и со службами по консультированию и информированию для предотвращения других возможных ситуаций жестокого обращения в Интернете во время дистанционных уроков, включая онлайн или вне уроков.

с. Педагог узнает о подозрительном случае онлайн-насилия над ребенком, не связанном с дистанционным образовательным процессом²;

² При классификации случаев онлайн-насилия учитывались категории серьезности буллинга, изложенные в исследовании Буллинга среди подростков Республики Молдова, проведенном Институтом социальных технологий «Социополис» по просьбе ЮНИСЕФ Молдова, Кишинэу, 2019 г.

Менее серьезный случай насилия в Интернете

- Распространение отредактированных фотографий ребенка, мамы которые выставляют в плохом свете;
- Публикация неприятных комментариев к постам ребенка в социальных сетях со стороны коллег или сверстников;
- Получение неприятного сообщения от кого-либо и т.д.

Педагог предпримет следующие действия:

1. Проведет беседу с учеником, который прошел через этот опыт насилия;
2. Посоветует/поможет ребенку сообщить о комментарии, фотографии, неприятном контенте на веб-платформе, на которой он был опубликован, и заблокировать пользователя/пользователей, которые ведут себя неадекватно, если они являются посторонними;
3. Уведомит о соответствующей ситуации администрацию учебного заведения/ответственное лицо, назначенное учреждением;
4. Проведет конструктивную беседу с другими учениками, вовлеченными в эту ситуацию. Сообщит родителям ребенка, подвергшегося насилию, о совершенных в отношении него действиях, их последствиях, мерах, предпринятых сотрудниками учебного заведения, обратит внимание родителей, чтобы не наказывать ребенка и не обвинять его, а наоборот помочь ему преодолеть эту ситуацию;
5. Будет наблюдать/оценивать поведение и эмоциональное состояние ребенка/детей;
6. Если инициатором насилия является ребенок из того же класса, он также пообщается с этим учеником и его родителями в соответствии с процедурами, применимыми в случаях насилия в учебном заведении;
7. При необходимости пригласит психолога для работы с ребенком/детьми, вовлеченными в ситуацию.

Случай средней тяжести насилия в Интернете

- В Интернете, в социальных сетях распространялась ложь, сплетни, уничижительные высказывания в адрес ребенка;
- Ребенок получает оскорбительные сообщения от известных или неизвестных лиц или из фейковых аккаунтов;
- Публикация без согласия ребенка интимных фотографий (например, в нижнем белье или в купальнике);
- Были созданы фейковые аккаунты с использованием персональных данных ребенка;

Педагог предпримет следующие действия:

1. Проведет беседу с учеником, который прошел через этот опыт насилия;
2. Уведомит администрацию учебного заведения и координатора мер по предотвращению, выявлению, информированию, направлению и помощи в случаях насилия в отношении детей;
3. Посоветует ребенку сообщать о контенте, опубликованном или распространяемом на веб-платформе;

4. Если ситуация связана со случаем буллинга или насилия в учебном заведении, он рассмотрит всех задействованных участников, в соответствии с процедурами, применимыми в случаях насилия в учебном заведении;
5. Сообщит родителям ребенка, подвергшегося насилию, о совершенных в отношении него действиях, их последствиях, мерах, предпринятых сотрудниками учебного заведения, и попросит родителя не наказывать ребенка и не обвинять его, а наоборот помочь ему преодолеть эту ситуацию;
6. При необходимости будет задействован психолог в работе учениками/детьми, вовлеченными в ситуацию.
7. В случае необходимости он обратится к службе защиты детей и социальные службы.

Серьезный случай насилия в Интернете

- Ему угрожали в Интернете, в социальных сетях, знакомые или незнакомые люди;
- В Интернете, в социальных сетях, над ребенком подшучивали, с неприемлемым подтекстом, или ребенок получал какие-либо комментарии, предложения или контент (видео или фотографии) сексуального характера;
- Публикация в онлайн-среде фотографий или видеороликов, представляющих ребенка в неприемлемых позах (без нижнего белья, имитация или участие в действиях сексуального характера и др.);
- Угроза или шантаж ребенка (sextortion) путем распространения компрометирующей информации о нем, в обмен на действия сексуального характера и др.

Педагог предпримет следующие действия:

1. Проведет беседу с учеником, который прошел через этот опыт насилия;
2. Немедленно уведомит администрацию учреждения и координатора мер по предотвращению, выявлению, информированию, направлению и помощи в случаях насилия в отношении детей;
3. Школьный психолог подготовит план работы с учеником/классом, в котором сложилась данная ситуация.
4. Сообщит родителям ребенка, подвергшегося насилию, о совершенных в отношении него действиях, их последствиях, мерах, предпринятых сотрудниками учебного заведения, и обратит внимание родителей, чтобы не наказывать ребенка и не обвинять его, а наоборот помочь ему преодолеть эту ситуацию;
5. Проинформирует учеников и родителей о возможностях доступа к услугам психологической и медицинской помощи, личностного и социального развития и др.;
6. Учебное заведение будет сотрудничать с компетентными органами или/и со службами по консультированию и информированию для предотвращения других возможных ситуаций жестокого обращения в Интернете во время дистанционных уроков или вне уроков.

2.5 В условиях дистанционного образовательного процесса, в том числе онлайн, преподаватели будут применять те же принципы и правила общения с ребенком, который стал жертвой ситуации онлайн-насилия, что и в случаях насилия в образовательном учреждении.

III. Обеспечение защищённого доступа детей к веб-платформам и инструментам, используемым в дистанционном образовательном процессе;

3.1. В целях обеспечения безопасного доступа детей к веб-платформам и инструментам, используемым в дистанционном образовательном процессе, **руководитель учреждения** выполнит следующие действия:

- Порекомендует преподавателям использовать разрешенные/рекомендованные образовательные и коммуникационные платформы для образовательных целей;
- Организует обучение учителей мерам безопасности и конфиденциальности в рекомендуемых и используемых веб-платформах для образовательных целей, чтобы каждый преподаватель знал, как предотвратить ситуации, когда посторонние люди могут получить доступ к онлайн-урокам, заблокировать видео, аудио или чат и избежать доступа к своей персональной информации и персональной информации учеников в дистанционном образовательном процессе;
- В случае возникновения инцидента администрация учебного заведения проинформирует местный специализированный орган в области образования о незамедлительно предпринятых действиях /кто был проинформирован/;
- В результате инцидента учебное заведение:
 - проведет внутреннее расследование;
 - проведет беседы с детьми/родителями, с классным руководителем и психологом учреждения/специалистом Службы психолого-педагогической помощи (SAP);
 - сообщит Местным специализированным органам в области образования (OLSDI) о предпринятых мерах;
 - проинформирует детей о помощи, предоставляемой службой телефон доверия для детей 116111 (помещение телефона доверия для детей в учреждении), siguronline.md и 12plus.md;
 - обеспечит оформление и передачу местному органу опеки и попечительства уведомления о случае жестокого обращения, пренебрежения, эксплуатации или торговли ребенком, и копии этого уведомления координатору ANET, в случае, если оно в течение 24 часов не было передано в местный орган опеки и попечительства с указанием причины его непередачи.

3.2. Чтобы ограничить уязвимость с точки зрения безопасности деятельности в Интернете и снизить риски для безопасности и защиты детей, в процессе дистанционного обучения, **преподаватели** будут выполнять следующие действия:

- Использовать только разрешенные образовательные и дистанционные коммуникационные платформы в общеизвестных образовательных целях, загруженные с официальных сайтов.
- Тщательно изучать используемые приложения/платформы, все варианты, которые они предлагают.
- При планировании онлайн-сеанса преподаватели будут устанавливать функции безопасности используемой платформы: идентификатор конференции, пароль доступа, блокировку нежелательного доступа и т.д.
- Приглашение к участию, содержащее ссылку для входа, идентификатор сеанса и пароль, будут отправлены только по защищенному каналу связи.
- Они будут избегать общения с учениками на социальных платформах (например, Facebook, Instagram, Odnoklassniki и т.д.) и будут использовать только специально созданные для этой цели группы на платформах, используемых для образовательных целей (например, Инструменты Google для образования в пакете G Suite).

- Установят пароль для каждого онлайн-сеанса с учениками, чтобы предотвратить несанкционированный доступ.
- Следить за разговорами в общем чате и в случае неуместных обсуждений, незамедлительно вмешаются, остановив/заблокировав чат и покинув платформы. В случае выявления ситуации травля в онлайн среде во время онлайн-урока будут применены рекомендации, указанные в пункте III.
- Подключение к онлайн-сеансу будет осуществляться за несколько минут до него. Не допускается подключение учеников до учителя. Если приложение позволяет, будет активироваться опция Waiting Room (зал ожидания). Эта функция позволяет организатору (учителю) контролировать, когда или какой участник присоединяется к сессии. В качестве организатора сессии учитель может принимать или исключать участников одного за другим.
- В начале сессии преподаватель будет проверять личность каждого участника, а в случае неизвестного участника его участие будет отклонено.
- Если в сессии появилось незнакомое лицо, которое мешает воспроизведению видео и звука во время урока, то сразу же будут заблокированы все микрофоны и видеорекамеры, а сессия будет остановлена. О любом подобном инциденте необходимо сообщать руководству учреждения/лицу, назначенному руководством учебного заведения.
- Как администратор сессии, преподаватель может включать/выключать изображения подключенных участников. Для относительно небольшой группы участников, например учеников в классе, можно оставить активные видеорекамеры.
- Если записан урок, который будет доступен в Интернете, видеорекамеры будут деактивированы, преподаватель проследит, чтобы никакие личные данные не отображались.
- Участникам не разрешается записывать сессию. Ученикам сообщается о том, что только преподаватель может контролировать запись, которая затем будет передана всем заинтересованным сторонам.
- По завершении урока преподаватели не будут закрывать сеанс, пока не убедятся, что все ученики, участвующие удаленно, отключатся от коммуникационной платформы.
- Ответственным образом вести списки имен и адресов электронной почты учеников.
- Списки учеников с персональными данными будут храниться только на оборудовании, оснащенном всеми функциями безопасности.
- Никакие списки с персональными данными не будут отправлены в виде незапароленных вложений электронной почты.
- Преподаватели объяснят ученикам, что следующие действия в Интернете по отношению к ребенку являются жестоким обращением и попросят учеников сообщать о соответствующих случаях, когда:
 - человек ведет дискуссии неприемлемого или интимного содержания с учениками, либо через текстовые сообщения, либо через аудиосообщения/видеосообщения, либо через аудиозвонки/видеозвонки, или другими способами;
 - человек просит ребенка прислать интимные фотоизображения/видеоизображения, независимо от того, получает ли он их или нет;
 - человек передает ребенку фотоизображения/видеоизображения неприемлемого характера или ссылки на такой контент;
 - человек призывает или навязывает ребенку действия неприемлемого или интимного характера, либо в виртуальной среде, либо просит о физической встрече с той же целью;
- Преподаватели объяснят ученикам, чтобы они не сообщали посторонним в Интернете свое имя, адрес, номер телефона, данные из своего аккаунта в социальных сетях или другие персональные данные;

- Объяснят ученику, что в случае жестокого обращения в Интернете он может проконсультироваться бесплатно, в том числе анонимно, следующим образом:
 - Телефон ребенка: 116-111
 - Веб-сайт: <https://siguronline.md>, <https://12plus.md/>

Преподавателям рекомендуется изучить *Руководство для профессионалов «Что такое сексуальная эксплуатация детей в Интернете»*, разработанное Международным Центром «La Strada», ресурсы, размещенные на сайте Министерства образования, культуры и исследований <https://mecc.gov.md/ro/content/siguranta-copiilor-internet>, учебники по *Медиаобразованию* на платформе <https://educatia.mediacritica.md/ro/>, а также другие ресурсы, доступные на сайте <https://siguronline.md>.

Если был идентифицирован неизвестный человек/произошел инцидент, связанный с нарушением работы класса, злоупотребление уязвимости детей в Интернете, преподаватель СООБЩАЕТ об этом следующим образом:

- Сообщает об инциденте администрации учреждения/ответственному лицу, назначенному руководством учебного заведения;
- Уведомляет компетентные органы одним из следующих способов:
 - По телефону: 116-111; (022) 577-177; 112;
 - По e-mail: diii.ini@igp.gov.md
 - веб-сайты: siguronline.md, 12plus.md, politia.md

ВНИМАНИЕ! Несообщение о случаях жестокого обращения в Интернете способствует тому, что злоумышленник подвергает детей виктимизации. За ребенком-жертвой всегда есть и другие дети, подвергшиеся жестокому обращению.

3.3. Преподаватели проведут беседу с учениками о веб-платформах, используемых во время дистанционного обучения, сославшись на следующие аспекты:

- a. *Их функциональность* (как работает платформа, и для каких целей она будет использоваться);
- b. *Необходимые и обязательные настройки безопасности*
 1. Ученики будут предупреждены о том, что нельзя открывать подозрительные ссылки или прикрепленные документы, даже если они были отправлены друзьями, поскольку они могут содержать вирусы, шпионские или вредоносные программы на компьютере, что ставит под угрозу его безопасность.
 2. Родителям будет предложено проверить, есть ли у них антивирусные программы или какое-либо программное обеспечение для обеспечения безопасности в Интернете, установленное на цифровых устройствах, используемых ребенком в дистанционном образовательном процессе.
 3. Ученикам и родителям объяснят, как проводить удаленный урок и создать учетную запись для ребенка, обратив их внимание на персональные данные, которые они могут указать на веб-платформе.
- c. *Способы подключения к учебному процессу/онлайн-уроку через платформу/платформы*

Например: Перед тем как отправить ссылку на онлайн-урок, преподаватели задумаются над такими вопросами: Кому отправить ссылку и как ее отправить. Кто видит эту ссылку, чтобы не допустить, чтобы она попала к посторонним лицам. Как ученик подключается и передает ли ученик ссылку другому лицу, например, однокласснику или родственнику одноклассника. К кому обращается ученик, если

он не может подключиться? К кому обращается преподаватель, если у него есть проблемы технического характера?

d. Четкие правила использования платформы во время онлайн-учебы

Например, кто показывает экран, кто разрешает доступ к уроку на платформе. Кто и для чего используется чат платформы. Кто может покинуть урок, и по каким причинам. Имя, с которым подключается каждый участник. Преподаватель возьмет на себя ответственность за то, чтобы быть модератором платформы, которая разрешает или ограничивает доступ к учебному процессу, разрешает демонстрацию экрана, решает, кто покидает платформу во время урока и т. д.

3.4. Местные специализированные органы в области образования будут выполнять следующие действия:

- запросят информацию о подобных инцидентах, которые произошли у них с момента объявления чрезвычайного положения в связи с пандемической ситуацией COVID-19.
- организуют/будут сотрудничать с партнерами в целях обучения преподавателей по
 - обеспечению безопасной виртуальной среды для детей;
 - кибербезопасности;
 - устранению вновь выявленных рисков;
 - работе с детьми/взаимодействию/участию психолога/специалиста SAP;
 - работе с родителями/законными представителями;
 - предотвращению случаев буллинга.
- предложат регулярное обсуждение темы насилия в отношении детей на повестку дня районного/муниципального совета по защите прав ребенка в целях выявления и решения проблем межсекторального сотрудничества.

3.5. Координатор ANET:

- будет собирать информацию об инцидентах, произошедших в онлайн-среде:
 - на уроках, проведенных в режиме онлайн;
 - вне уроков, но относящихся к инцидентам, связанным с безопасностью ребенка в онлайн-среде;
- составит/отправит файл уведомления о предполагаемом случае насилия, пренебрежения, эксплуатации и торговли ребенком, подготовленный учебным заведением, в местный / территориальный орган опеки и попечительства для регистрации и принятия мер, необходимых для оказания помощи ребенку;
- сообщит Министерству образования, культуры и исследований об инциденте и немедленных действиях, предпринятых в течение 3 рабочих дней.

IV. Технические аспекты безопасного управления и блокирования попыток взлома онлайн-уроков

4.1. Безопасное использование приложения ZOOM

Организационные меры:


- Преподаватель создаст/начнет онлайн-урок (Zoom Meeting) используя личный аккаунт Zoom;

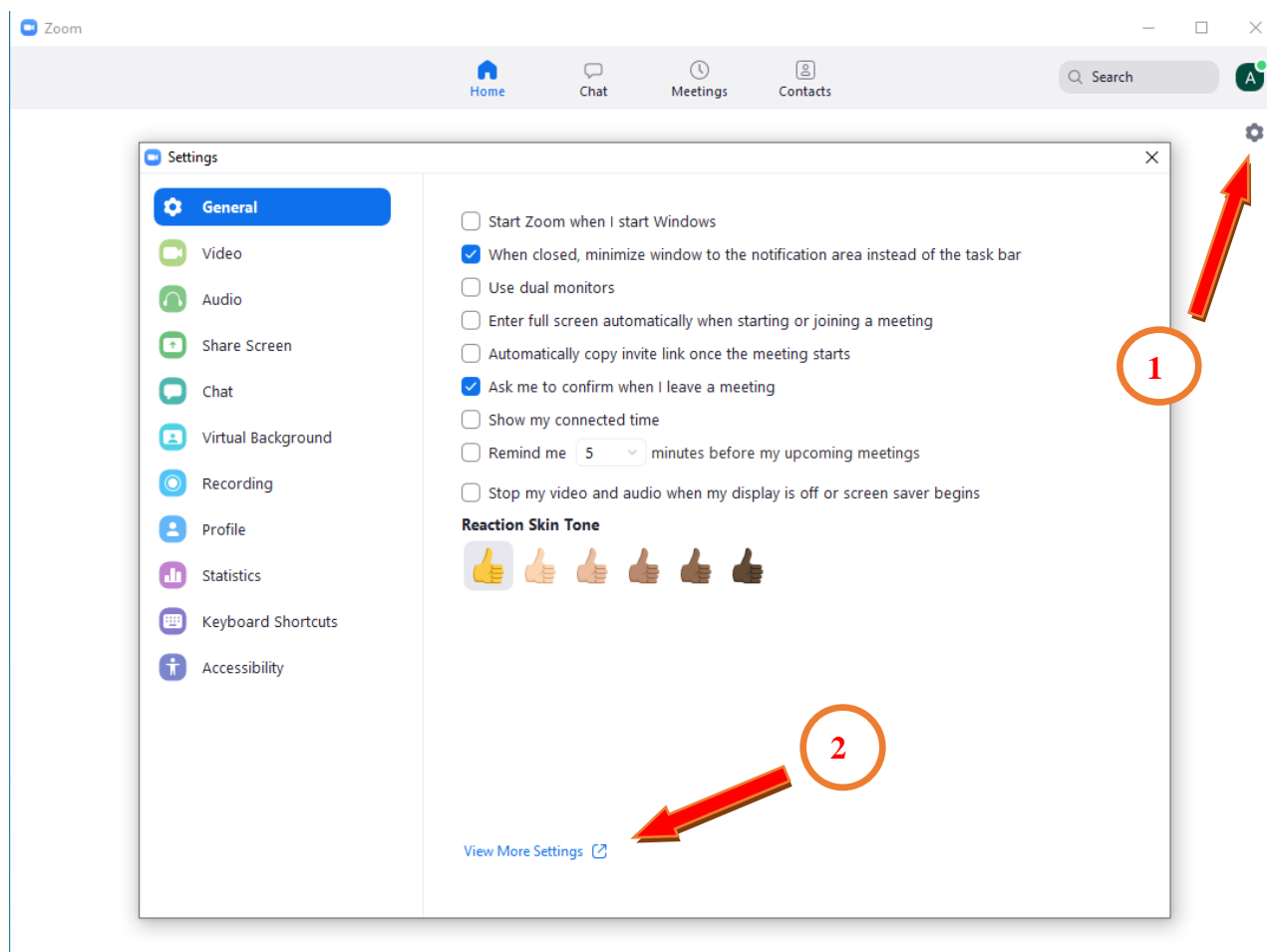
- Все участники онлайн-урока будут идентифицироваться реальными Фамилией+Именем, «никнеймы» не допускаются;
- Онлайн-урок (Zoom Meeting) **не** будет проводиться без присмотра преподавателя даже во время перерыва. По завершении урока или перерыва преподаватель остановит сессию (**End > End Meeting for All**), а после возвращения он перезапустит урок с повторным подключением всех учеников;
- Запрещается распространять ссылку на онлайн-урок (Zoom Meeting) неавторизованным лицам, в том числе тем, кого ученики знают лично.

Технические меры:

- Обновляем приложение – загружаем последнюю версию.
- Избегайте аутентификации через Facebook. Проблемы безопасности позволяют получить доступ к вашим персональным данным.

Настройки безопасности в приложении Zoom:

Чтобы установить некоторые параметры, обеспечивающие безопасность вашего онлайн-урока, перейдите в приложении Zoom в меню Настройки (символ зубчатого колеса ) > View More Settings > (откроется профиль в браузере)



В профиле приложения в браузере перейдите в меню Settings > Meeting > 1) Waiting Room > (Включить)

Объяснение: Когда участники подключаются к онлайн-уроку, они помещаются в список ожидания, и каждый из них принимается администратором (host). Включение списка

ожидания автоматически отключает подключение к уроку до того, как это сделает администратор (host).

- 1) Require a passcode when scheduling new meetings > **(Включить)**
Требуется ввести пароль для подключения участников.
- 2) Embed passcode in invite link for one-click join > **(Отключить)**
Отключение опции входа в систему, перейдя по ссылке без пароля.
- 3) Only authenticated users can join meetings from Web client > **(Включить)**
Подключение участников через веб-браузер возможно только после аутентификации в приложении Zoom.
- 4) Participants video > **(Включить)**
При входе в систему участник автоматически запускает видео, и видно, кто подключается.
- 5) Join before host > **(Отключить)**
Отключение подключения к онлайн-уроку до того, как это сделает администратор (host).
- 6) Sound notification when someone joins or leaves > **(Включить)**
(Отметить галочкой) Host and co-hosts only
Администратор получает уведомление при подключении/отключении участника.
- 7) Если вы не передаете файлы, то отключите функцию:
File transfer > **(Отключить)**
Никто не сможет передавать файлы в чат, включая администратора (host).
- 8) Если ученики не делятся своим экраном, тогда оставьте функцию активированной только для преподавателя («host»):
 - a) Screen sharing > **(Включить)**
(Отметить галочкой) Host Only > Save
 - b) Disable desktop/screen share for users > **(Включить)**
Только администратор может демонстрировать экран.
- 9) Remote control > **(Отключить)**
Отключение дистанционного управления участниками контента, показанного администратором.
- 10) Allow removed participants to rejoin > **(Отключить)**
Отключение возможности повторного подключения для пользователей, которые были удалены (отключены) из онлайн-урока администратором.
- 11) Report participants to Zoom > **(Включить)**
Администратор может сообщать приложению Zoom о неадекватном поведении участников. Этот параметр можно найти в значке безопасности (в виде щита) во время сессии Zoom (Zoom Meeting).

В профиле приложения в браузере перейдите в меню Settings > Recording >

- 1) Automatic recording > **(Включить)**
Онлайн-урок записывается автоматически. Запись будет сохранена после завершения сессии Zoom. Выберите папку, в которой будет сохранен видеофайл.

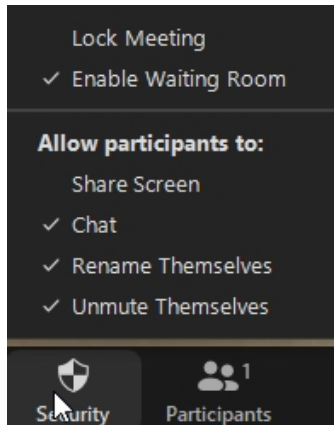


Convert Meeting Recording

You have a recording that needs to be converted before viewing.

33%

Stop Converting



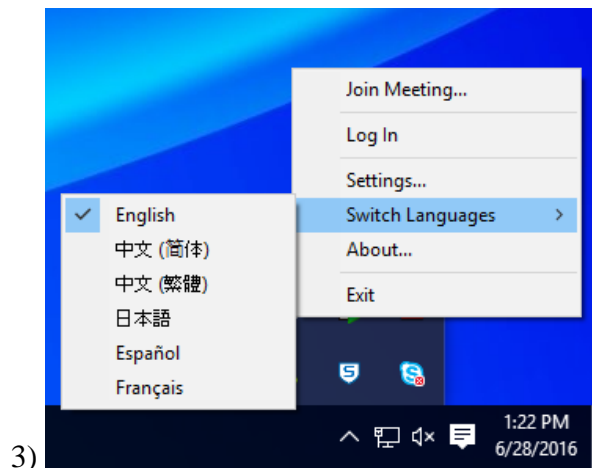
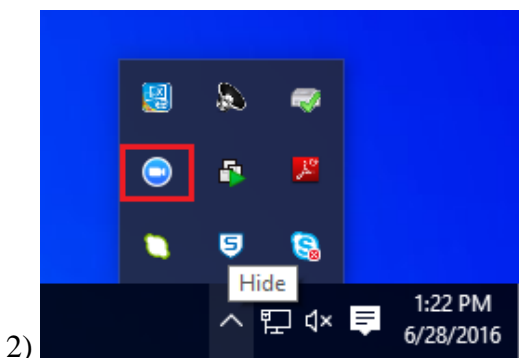
Во время видео-сессии – в меню «Security»:

1) Проверяем, чтобы было (отмечено галочкой) Enable Waiting Room
(Список ожидания включен)

2) если ученики не делятся своим экраном:

Проверяем, чтобы было (снять галочку) Share Screen

Выбор языка для приложения Zoom:



2.2. Безопасное использование приложения Google Meet

Элементы управления безопасностью Google Meet включены по умолчанию, поэтому в большинстве случаев пользователям не нужно ничего делать, чтобы убедиться, что они должным образом защищены.

Внешние участники могут присоединиться к онлайн-сессиям, только если их внесли в список приглашенных или они приглашены участниками. В противном случае они

должны подать запрос на участие в онлайн-сессии, и их запрос должен быть принят организатором, то есть преподавателем.


Только администратор (организатор) может отключать или удалять других участников. Это гарантирует, что преподавателя не смогут удалить или отключить другие участники.

Только администратор (организатор) может одобрить запросы на участие, поданные внешними участниками. Это означает, что ученики не могут разрешить внешним участникам присоединяться через видео, а внешние участники не могут присоединиться к сессии.

Ученики не могут присоединиться к сессии после того, как ее покинул последний участник. Это означает, что если преподаватель покидает урок, то ученики не могут зарегистрироваться на него без присутствия преподавателя.

Организационные меры:

- Преподаватель инициирует онлайн-урок (Meeting) используя личный аккаунт Google;
- Все участники онлайн-урока будут идентифицированы через личный аккаунт Google, в котором указаны реальные Фамилия+Имя, «никнеймы» не допускаются;
- После получения от пользователя запроса на участие в уроке преподаватель убедится, что отображаемое имя присутствует в списке учеников класса. Сразу после подключения, участника попросят показать свое лицо для проверки личности;
- Запрещается распространять ссылку онлайн-урока (Meeting) неавторизованным лицам, в том числе тем, кого ученики знают лично.


 Необходимо учитывать, что в Google Meet, в отличие от приложения Zoom, если преподаватель (администратор) покидает урок, сеанс остается активным, и ученики могут остаться в нем без присмотра. Поэтому преподаватель должен покинуть онлайн-урок последним.


Меры безопасности в Google Meet:


1) Урок (Meeting) организуется путем создания ссылки:

 >  > Копируется ссылка (не допускается создание урока с немедленным доступом, нажав на иконку «+»)

2) В случае нарушения правил безопасного поведения, удалите участника:

Первый способ: Наведите курсор мыши на окно участника в Google Meet > Появится значок «» , на который вы должны нажать > В отображаемом окне подтвердите удаление участника;

Второй способ: В списке участников поместите курсор перед именем участника > Нажмите значок «стрелка вниз» (v) > Нажмите «» (Удалить)

3) Если участник начал демонстрацию экрана без разрешения, остановите ее: в списке участников поместите курсор перед опцией показа экрана участником (где указано имя участника и слово «демонстрация», взятое в скобках, в зависимости от языка отображения) > Нажмите значок «стрелка вниз» (v) > Нажмите «,» (Удалить).