СЕРВИЧИУЛ ПУБЛИК
ДЕ КУЛТУРЭ
ШИ ПАТРИМОНИУ ИСТОРИК АЛ
РЕПУБЛИЧИЙ
МОЛДОВЕНЕШТЬ НИСТРЕНЕ

ДЕРЖАВНА СЛУЖБА
З КУЛЬТУРИ
ТА ІСТОРИЧНОЇ СПАДЩИНИ
ПРИДНІСТРОВСЬКОЇ
МОЛДАВСЬКОЇ РЕСПУБЛІКИ

ГОСУДАРСТВЕННАЯ СЛУЖБА ПО КУЛЬТУРЕ
И ИСТОРИЧЕСКОМУ НАСЛЕДИЮ
ПРИДНЕСТРОВСКОЙ МОЛДАВСКОЙ РЕСПУБЛИКИ

МД 3300, г. Тирасполь, ул. 25 Октября, 96,
тел/факс 7-26-87, kultura_pmr@mail.ru

09.08.2021г. № 01-11/258

на №_____ от _____

И.о. ректора
ГОУ ВПО «Приднестровский
Государственный институт
искусств им. А.Г. Рубинштейна»
И.В. Плешкан

И.о. ректора
ГОУ ВПО «Бендерский высший
художественный колледж
им. В.И. Постойкина»
О.К. Рассадниковой

Уважаемая Ирина Владимировна!
Уважаемая Ольга Константиновна!

Государственная служба по культуре и историческому наследию Приднестровской Молдавской Республики направляет для использования в работе методические рекомендации Министерства цифрового развития, связи и массовых коммуникаций Приднестровской Молдавской Республики по обеспечению программной безопасности образовательного процесса с использованием дистанционных образовательных технологий.

Сообщаем о необходимости информирования профессорско-преподавательского состава учреждения с данными рекомендациями.

Приложение в электронном виде.

Начальник М.А. Кырмыз

Сапожник
053377122

Приложение 1

Информационная безопасность в образовательной организации

Важным требованием обеспечения деятельности образовательного учреждения является поддержание высокого уровня информационной безопасности (далее – ИБ). Причем ИБ здесь имеет свою специфику. Помимо **защиты баз данных** и предотвращения хакерских атак, важно оградить учащихся от любых проявлений пропаганды и манипуляций. Поэтому построение системы информационной безопасности в образовательной организации должны осуществлять специалисты, которые имеют соответствующий уровень квалификации и опыт.

Понятие ИБ в образовательной организации

Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. **Первой целью** является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц. **Вторая цель** ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

- персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;
- обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;
- защищенная законом интеллектуальная собственность.

Действия злоумышленников могут привести к хищению указанных данных. Также при несанкционированном вмешательстве возможны внесения изменений и уничтожение хранилищ знаний, программных кодов, оцифрованных книг и пособий, используемых в образовательном процессе.

В обязанности лиц, отвечающих за информационную безопасность, входит:

- обеспечение сохранности защищаемых данных;
- поддержание информации в состоянии постоянной доступности для авторизованных лиц;
- обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Также специалисты по ИБ обязаны не допустить несанкционированные изменения данных и их утрату.

Угрозы информационной безопасности

Спецификой обеспечения ИБ в информационных учреждениях является состав характерных угроз. К ним относится не только возможность хищения или повреждения

данных хакерами, но также деятельность учащихся. Подростки могут сознательно или ненамеренно повредит оборудование или заразить систему вредоносными программами.

Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

- компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия;
- программное обеспечение, применяемое в учебном процессе или для работы системы;
- данные, которые хранятся на жестких дисках или портативных носителях;
- дети и подростки, которые могут подвергаться стороннему информационному воздействию;
- персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер. К угрозам первого типа относятся:

- аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;
- программные сбои;
- ошибки работников;
- поломки оборудования;
- сбои систем связи.

Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации предсказуемы, достаточно эффективно и быстро устраняются подготовленным персоналом.

Намного более опасными являются угрозы информационной безопасности намеренного характера. Обычно результаты их реализации невозможно предвидеть. Намеренные угрозы могут исходить от учащихся, персонала организации, конкуренты, хакеры. Лицо, осуществляющее преднамеренное воздействие на компьютерные системы или программное обеспечение, должно быть достаточно компетентным в их работе. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Также внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание детей. Наиболее серьезная угроза – возможность вовлечения детей в криминальную или террористическую деятельность.

Способы несанкционированного доступа

Для хищения данных, создания нарушений в работе информационной системы и для других действий требуется несанкционированный доступ. Различают следующие виды несанкционированного доступа:

- **Человеческий**. Предусматривает хищение сведений методом их отправки по электронной почте или копирования на портативные носители, внесение вручную изменений в базы данных при наличии физического доступа к серверу.
- **Аппаратный**. Применение специального оборудования для хищения данных или внесения изменений в систему. В том числе может применяться оборудование для перехвата электромагнитных сигналов.
- **Программный**. Применение специального программного обеспечения для перехвата данных, копирования паролей, дешифровки и перенаправления трафика, внесения изменений в функционирование другого софта и т. д.

Меры защиты

Современные технологии информационной безопасности образовательной организации предусматривают обеспечение защиты на 5 уровнях:

- *нормативно-правовой;*
- *морально-этический;*
- *административно-организационный;*
- *физический;*
- *технический.*

1. Нормативно-правовой способ защиты

1. Основным документом, определяющим степень угроз и меры обеспечения информационной безопасности обучающихся в образовательной организации, является «Национальная стратегия действий в интересах детей». Она предусматривает приоритет мер, направленных на защиту сознания ребенка от информационного воздействия агрессивного характера. Меры по защите информационных систем и баз данных имеют второй уровень приоритетности.

Законодательством определяются данные, которые должны быть защищены от несанкционированного доступа третьих лиц. К числу таких сведений относятся:

- персональные данные;
- конфиденциальные сведения;
- служебная, профессиональная, коммерческая тайна.

Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом, Гражданским кодексом, Федеральным законом «Об информации» и другими актами. Конкретные меры по защите данных, используемое для этого аппаратное и методическое обеспечение определяются законами и профильными ГОСТами.

2. Морально-этические средства обеспечения информационной безопасности

Система морально-этических ценностей имеет особое значение в сфере образования. Она служит основой для выработки комплекса мер, направленных на защиту детей и подростков от информации этически некорректного, травмирующего, противозаконного характера. Защита детей от пропаганды основывается на законе «О защите прав ребенка». Этим актом определяются права детей на защиту от информации, которая может стать причиной моральной травмы.

В рамках мер по обеспечению ИБ создаются перечни источников (программ, документов и т. д.) способных травмировать детскую психику. В результате принимаемых мер должен предотвращаться доступ таких источников на территорию образовательного учреждения.

3. Меры административно-организационного характера

Система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

- должностные инструкции;
- внутренние методики по ИБ;
- перечни не подлежащих передаче данных;
- регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными методиками должен определяться порядок доступа учеников в интернет во время занятий в компьютерных классах, меры по предотвращению доступа детей к определенным ресурсам, предотвращение использования ими своих носителей информации и т. д.

4. Физические меры

Ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет непосредственно руководитель образовательной организации и ее IT-персонал. Не допускается перекладывание этих мер на наемные охранные структуры.

К числу физических мер относятся:

- реализация пропускной системы для доступа в помещения, в которых находятся носители данных;
- создание системы контроля и управления доступом;
- определение уровней допуска;
- создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.

Также среди физических мер можно назвать правила по созданию паролей и их периодической замене.

5. Технические меры

Технические меры защиты предусматривают использование специализированного программного обеспечения. В том числе в образовательных организациях рекомендуется использовать DLP и SIEM-системы, которые эффективно обнаруживают угрозы ИБ и обеспечиваю борьбу с ними. При невозможности использования подобных систем по причине бюджетных ограничений, применяются рекомендованные и разрешенные антивирусы и другие виды специального софта.

Приложение 2

Предложения по обеспечению программной безопасности образовательного процесса во время видеоконференций посредством системы Zoom.

Как защитить свои собрания Zoom от взлома

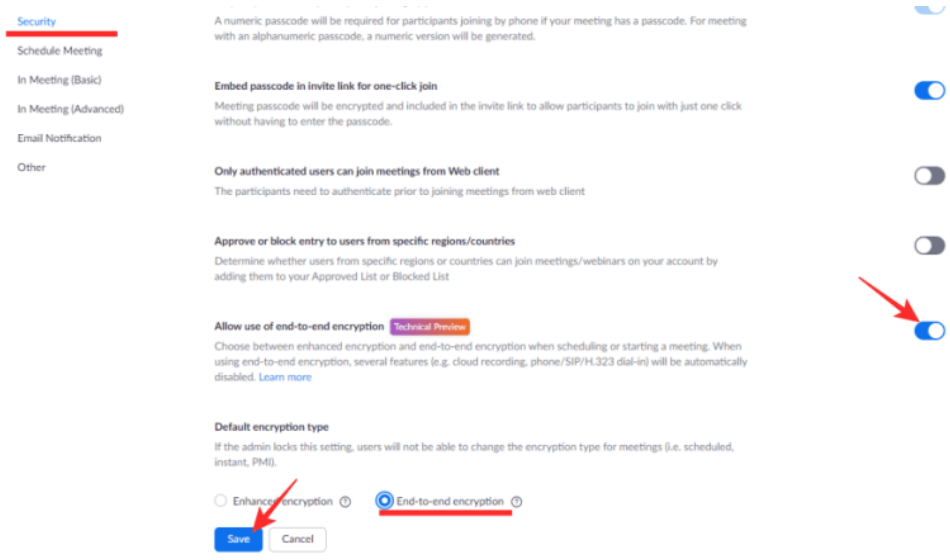
С ростом числа людей, внезапно работающих из дома, собрания Zoom стали почти образом жизни. Будь то для использования в офисе, в образовании или просто для друзей и семьи, количество пользователей этого приложения резко возросло. Zoom прост в использовании и доступен на всех основных платформах, что делает его одним из популярных приложений для многих.

Однако растущие опасения по поводу безопасности и конфиденциальности привели к тому, что приложение попало под микроскоп. Zoom разработал план по повышению своей безопасности, но пока вот что мы можем сделать, чтобы наши вызовы Zoom были настолько безопасными, насколько мы можем их сделать.

Как масштабировать встречу: настройка, присоединение, организация, планирование и многое другое

Включить сквозное шифрование

Сквозное шифрование широко называют золотым стандартом шифрования и безопасности. Этот протокол шифрования гарантирует, что никому, кроме тех, кто общается, не разрешено читать ни одного бита передаваемых данных. Zoom столкнулся с множеством критических замечаний за то, что он не соответствовал требованиям с точки зрения шифрования, и это новое дополнение – подходящий ответ сомневающимся. Эта функция все еще находится в стадии бета-тестирования, и вы упустите облачную запись, телефонный / SIP / H.323-вход и многое другое, но это по-прежнему лучший способ обеспечить безопасность отраслевого уровня. **Чтобы включить сквозное шифрование, перейдите в «Настройки», затем «Безопасность» и, наконец, включите «Разрешить использование сквозного шифрования».** Вам будет предложено ввести свой номер телефона и код подтверждения. В конечном итоге вам нужно установить тип шифрования по умолчанию на «Сквозное шифрование» и нажать «Сохранить».

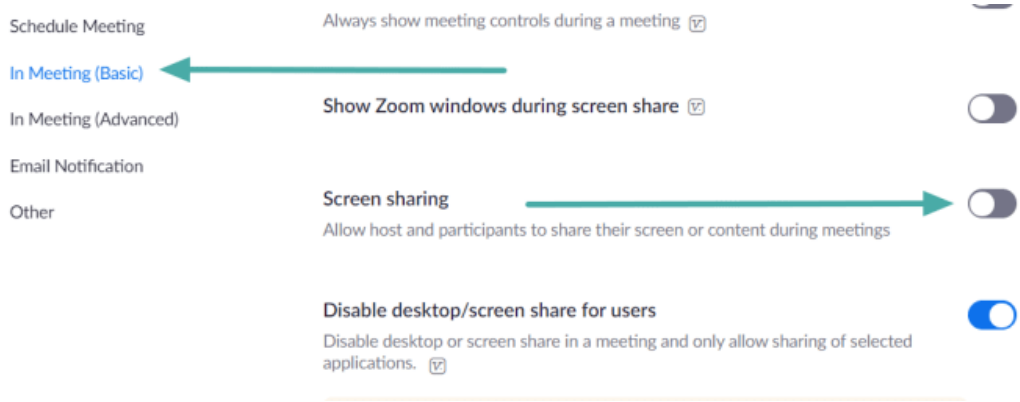


Частный идентификатор

Это очевидный вопрос. Воздержание от публикации идентификаторов собрания в публичных форумах и вместо этого отправка их непосредственно участникам снизит шансы незнакомых людей найти вашу встречу. Это особенно полезно, если вы уже знаете свой список участников встречи.

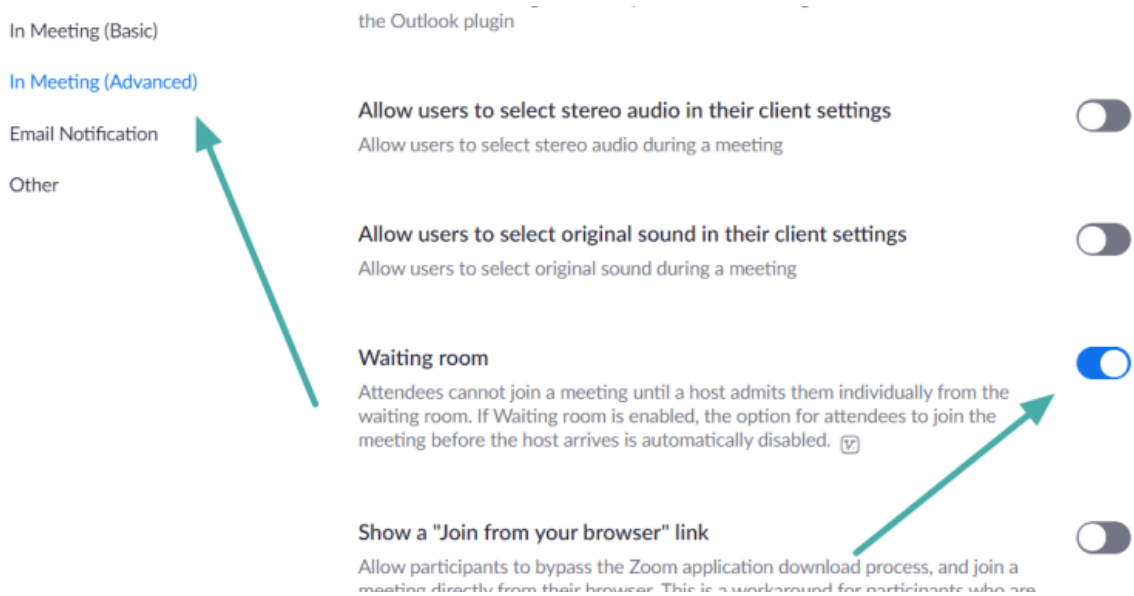
Да, это не всегда возможно, особенно когда это публичное мероприятие, такое как вебинар. В таких случаях наличие предполагаемого «Запроса» идентификатора помогает отслеживать, кто получил идентификатор встречи.

Совместное использование экрана



Совместное использование экрана позволяет пользователям делиться своими личными экранами со всеми участниками собрания. Поскольку нет способа ограничить то, чем можно делиться на экране, было множество сообщений о том, что на собраниях публиковались оскорбительные материалы.

Залы ожидания



Понимая, что не всегда можно сохранить конфиденциальность идентификатора переговорной комнаты, Zoom представил «Залы ожидания». Этот дополнительный элемент безопасности предназначен для удержания нежелательных пользователей от встречи.

По умолчанию залы ожидания Zoom включены, но если вам нужно найти настройку самостоятельно, вы можете найти ее под *Настройки* вкладка > *На собрании (расширенный)*> *Зал ожидания.*

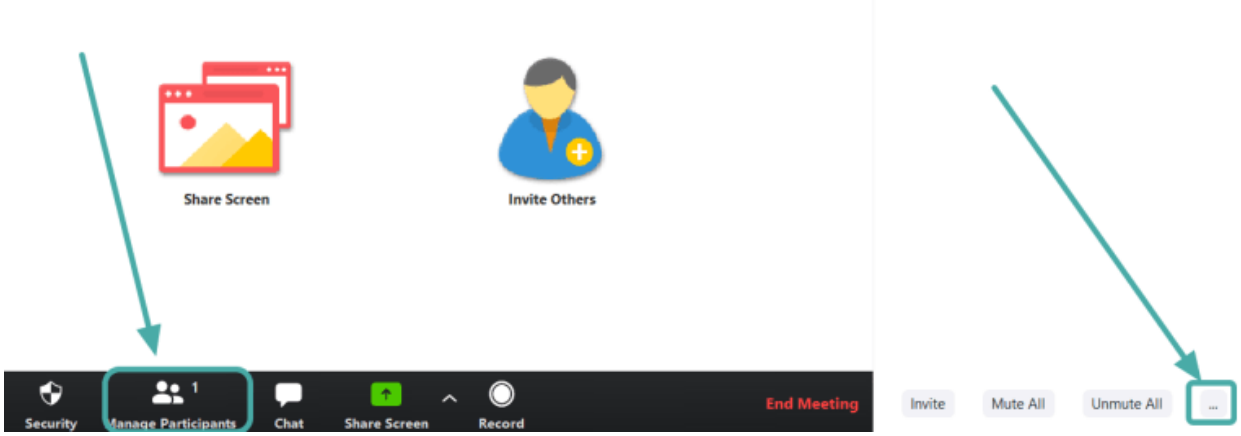
Однако, чтобы отключить комнаты ожидания, вы должны убедиться, что ваши собрания защищены паролем. Zoom позаботился о том, чтобы у пользователей была включена либо комната ожидания, либо пароль для дополнительной безопасности.

Заблокировать встречу

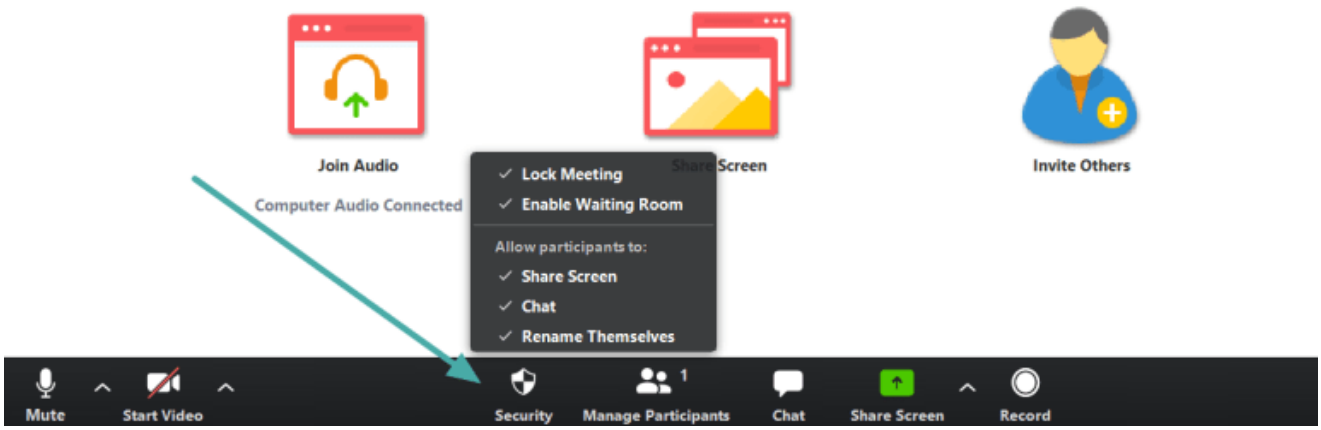
Как упоминалось выше, еще один способ проникновения пользователей на собрание – это циклическое переключение идентификаторов собрания до тех пор, пока они не найдут активный. Эта дополнительная функция безопасности устраняет эту угрозу. Чтобы не допустить незваных пользователей, достаточно просто заблокировать встречу после того, как все участники прибудут.

Однако с другой стороны, после того, как собрание заблокировано, даже пользователи, у которых есть пароль, не смогут войти в него. Поэтому перед блокировкой собрания лучше убедиться, что все присутствуют.

Выберите *Управлять участниками* в нижней части экрана, затем нажмите на 3 маленькие точки в правом углу. Выбирать *Заблокировать встречу*, и вы сделали!



Доступ к большинству из этих настроек безопасности, упомянутых выше, можно получить из *Безопасность* вкладка в нижней части экрана вызова.

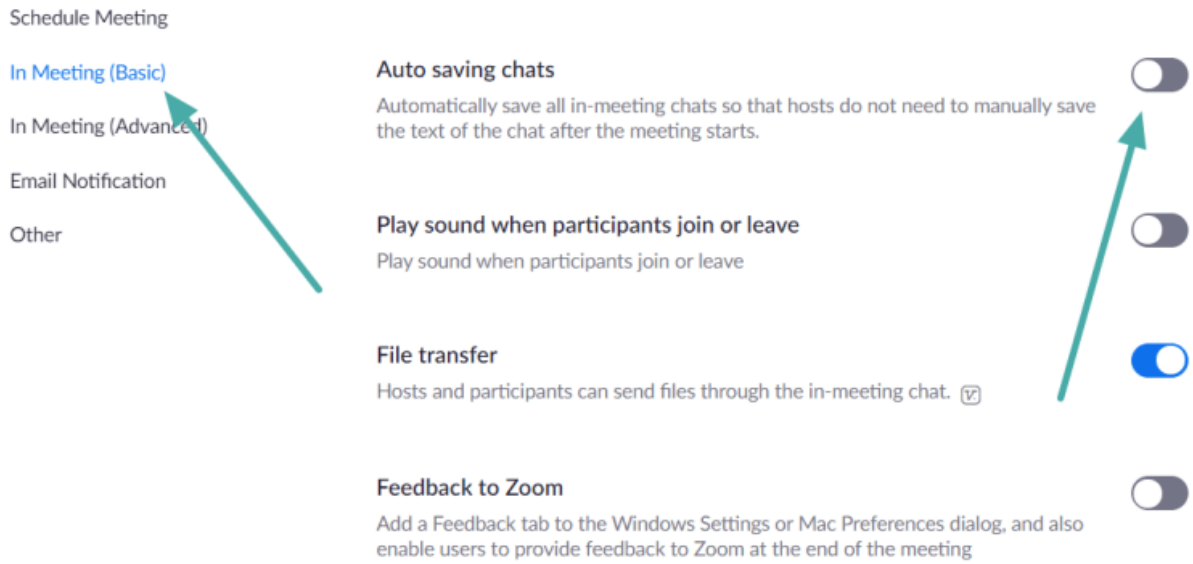


Отключить автосохранение чатов

Следуя идее исчезновения чатов, Zoom позволяет пользователям включать / выключать эту опцию. Если ваша встреча является конфиденциальной, и вы не хотите, чтобы кто-либо сохранял чаты, которые происходят во время встречи, рекомендуется отключить функцию автосохранения Zoom.

Выключение функции по-прежнему позволяет организатору сохранять чаты в собрании, когда они этого пожелают, но предотвращает сохранение чатов ВСЕХ собраний по умолчанию.

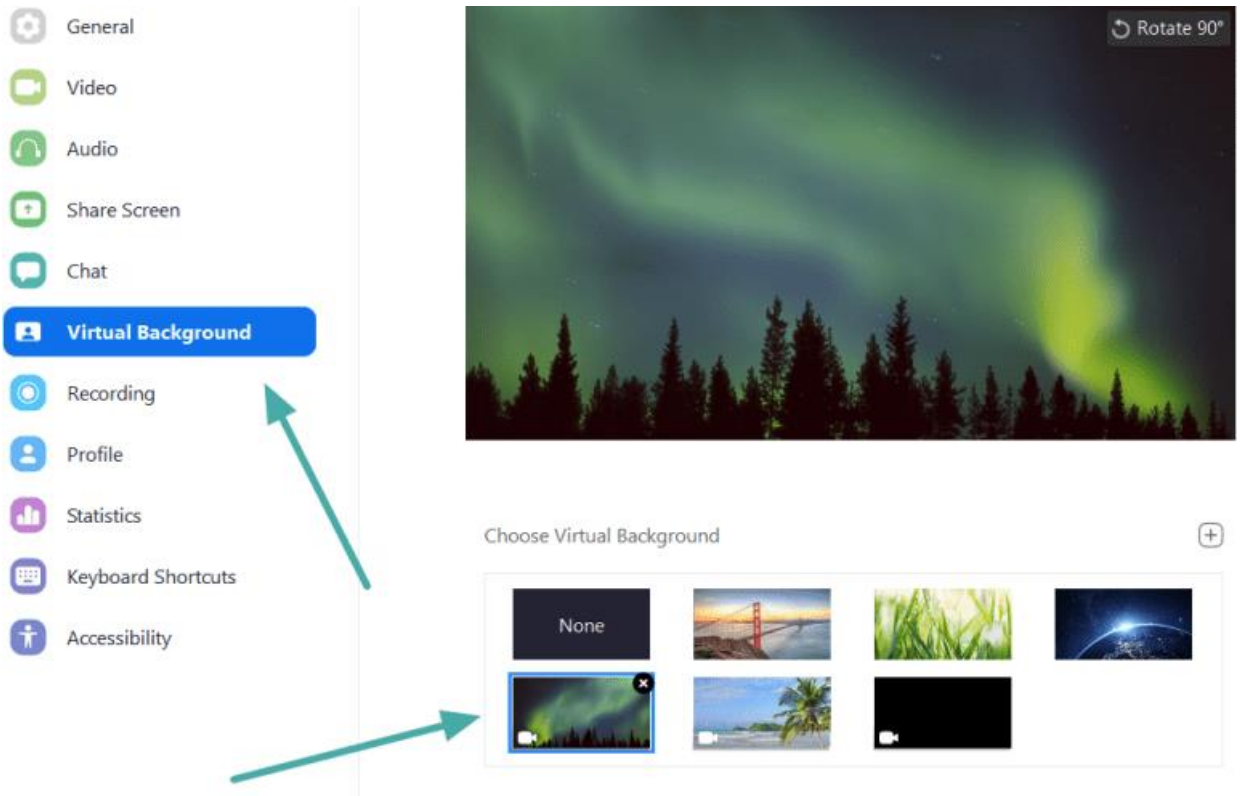
На вкладке настроек выберите *Встреча (базовая)* и переключить *Автосохранение чатов* к **ВЫКЛЮЧЕННЫЙ.**



Виртуальные изображения / видео фоны

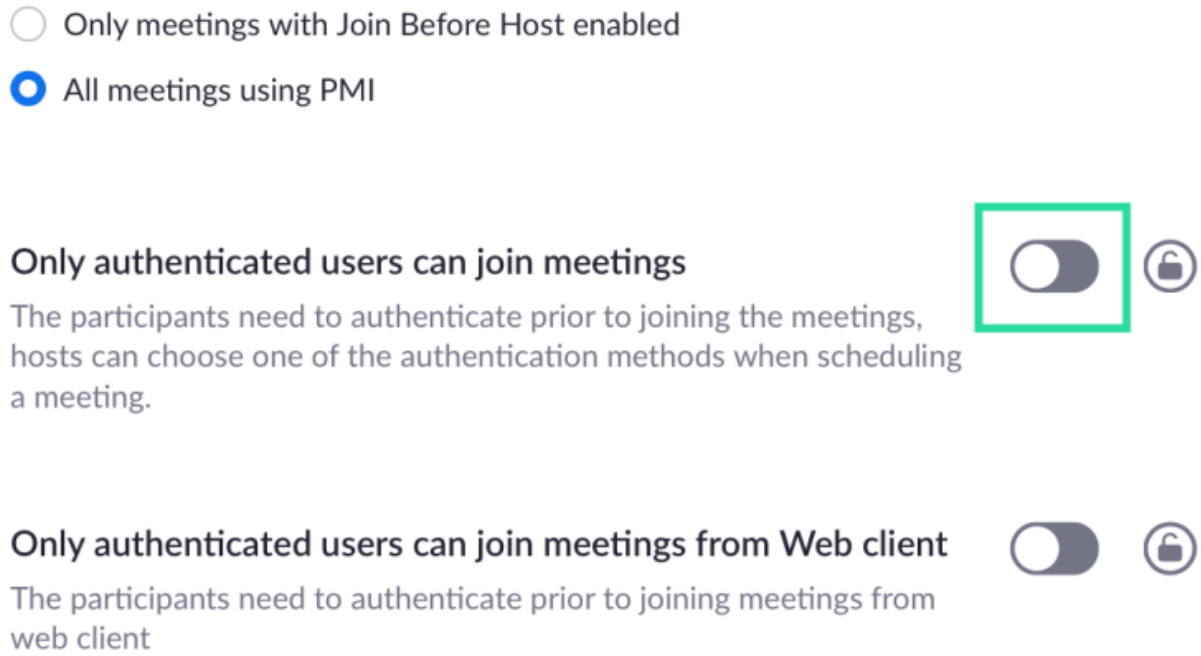
Чтобы защитить индивидуальность вашей «домашней» рабочей среды, Zoom позволяет пользователям накладывать себя на виртуальный фон, тем самым устраняя любой фоновый шум. Каким бы забавным это ни казалось, это помогает пользователям получить немного больше конфиденциальности при работе из дома.

Щелкните значок настроек в правом верхнем углу приложения Zoom и выберите *Виртуальные фоны* таб. Здесь вы можете выбирать между фоновыми изображениями и виртуальными фоновыми изображениями.



Чтобы узнать больше об изменении виртуального фона, ознакомьтесь с нашей статьей.

Разрешить только аутентифицированным пользователям присоединяться к собраниям

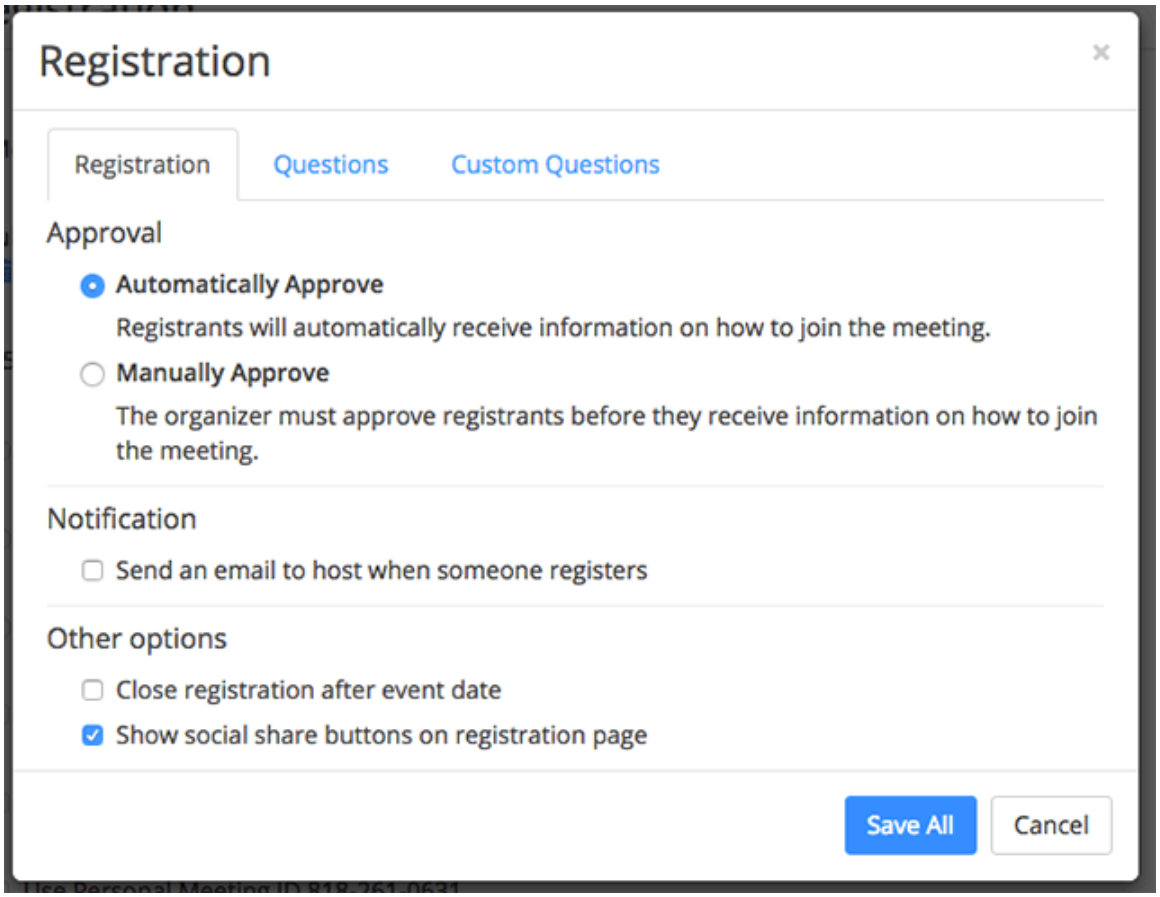


Zoom предлагает возможность создавать профили аутентификации, которые позволяют организаторам решать, какой участник может присоединиться к собранию. Как администратор, вы можете включить опцию добавления только аутентифицированных пользователей для входа в сеанс собрания, перейдя в Настройки учетной записи и

включение опции рядом с «Только аутентифицированные пользователи могут присоединяться к собраниям».

Вы можете выбрать один из двух методов аутентификации – Войти в Zoom и Войти в Zoom с указанными доменами. «Войти в Zoom» можно выбрать, если вы хотите разрешить на собрание всех, кто вошел в свою учетную запись Zoom. При выборе опции «Войти в Zoom с указанными доменами» только пользователи с определенными доменами смогут присоединиться к собранию.

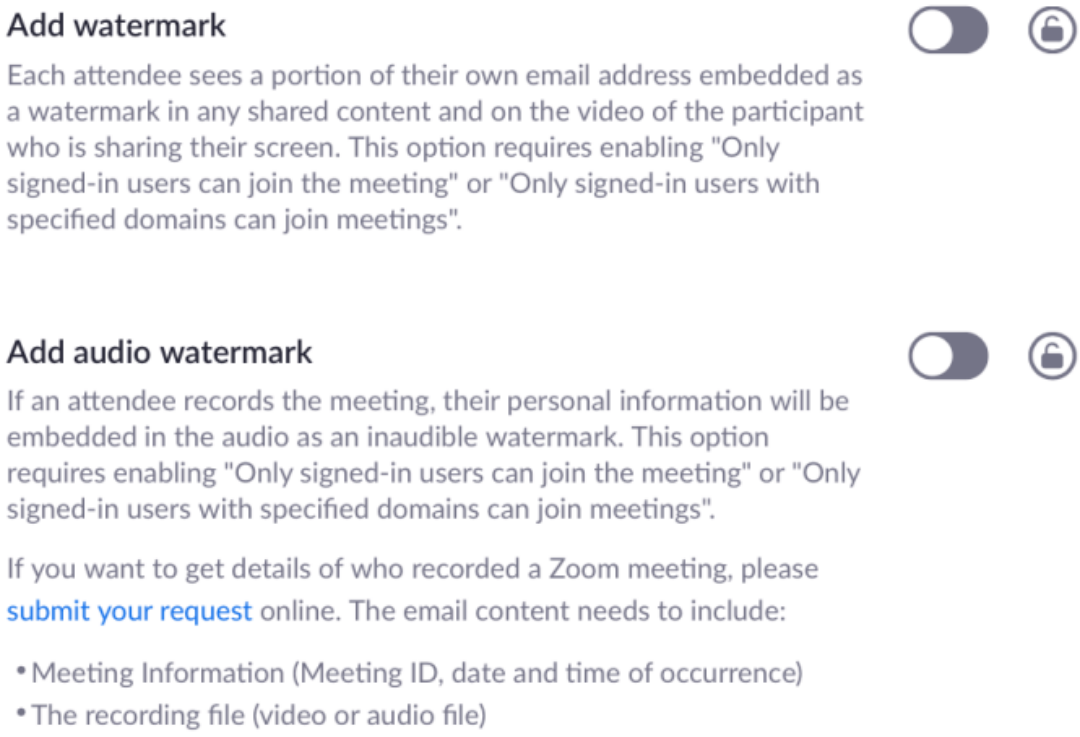
Требовать регистрацию для участников



В дополнение к созданию профилей аутентификации Zoom также позволяет вам требовать регистрацию от пользователей, которые хотят присоединиться к вашей встрече. Если для встречи требуется регистрация, участники должны будут указать свой адрес электронной почты, имя и ответить на вопросы, заданные им организатором. Чтобы включить требование регистрации, организатор встречи должен быть лицензированным пользователем, то есть он должен использовать любой из платных планов Zoom.

Вы можете установить флажок «Регистрация: требуется» при планировании собрания, чтобы решить, хотите ли вы утверждать участников при регистрации или после того, как вы разрешите им это. Затем вы можете перейти к выбору вопросов или разработке собственных вопросов, чтобы задать их любому, кто подписался на участие в собрании.

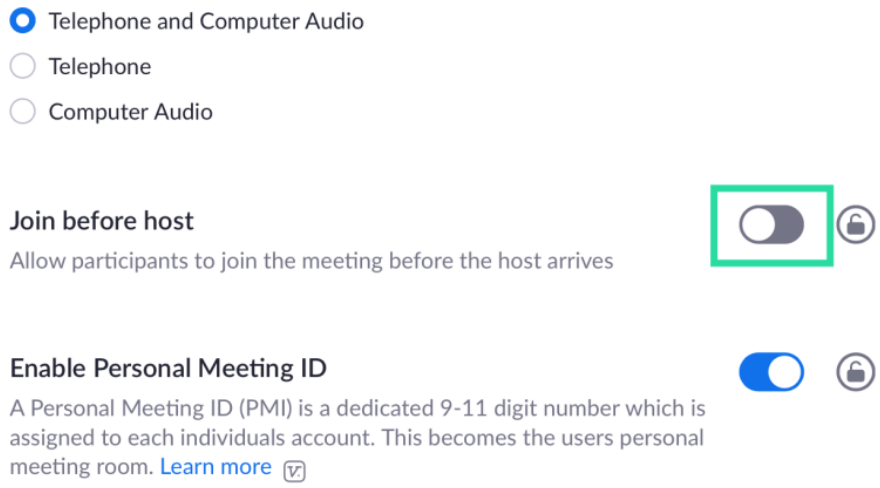
Включите водяные знаки с изображениями и звуком для ваших встреч



Чтобы защитить информацию, которая передается во время сеанса встречи в Zoom, вы можете добавить водяные знаки в свой видеопоток, общие экраны и звук. Водяные знаки в Zoom доступны в Zoom двумя разными способами – изображения и аудио.

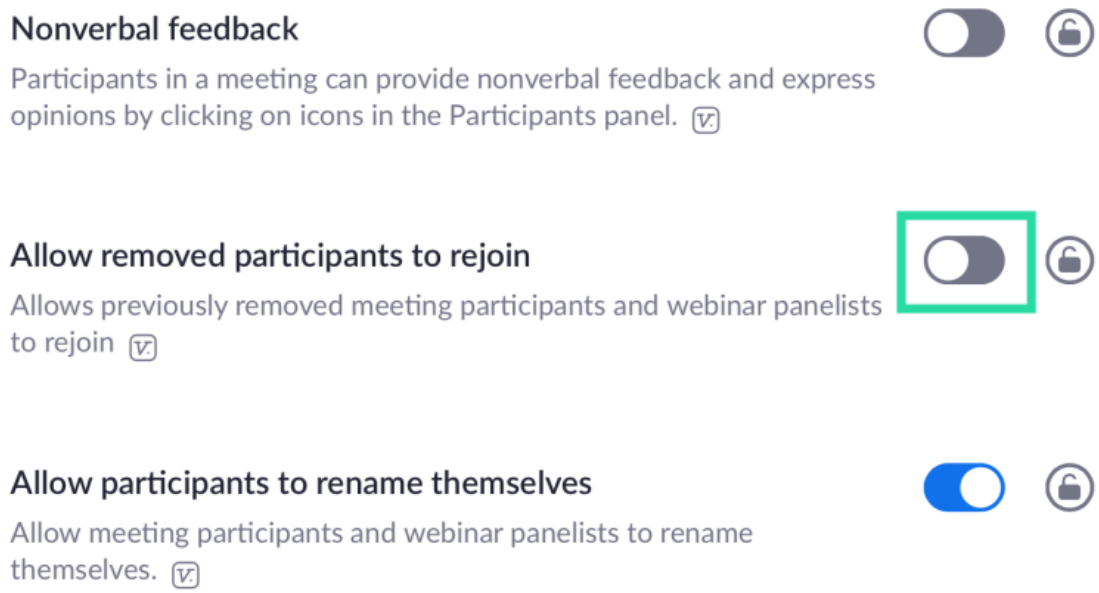
Если вы показываете свой экран другим участникам собрания, часть вашего адреса электронной почты будет отображаться на вашем общем экране, а также в ленте видео. С помощью звуковых водяных знаков Zoom установит неслышимый звуковой сигнал, содержащий вашу личную информацию, чтобы помочь определить, записал ли участник встречу. Вы можете включить водяные знаки с изображениями и звуками, перейдя в Настройки учетной записи на Zoom.

Отключить присоединение перед хостом



Zoom позволяет организаторам разрешить участникам присоединиться к собранию до того, как они войдут в него сами. Хотя разрешить другим участникам присоединиться до того, как хост станет удобным, это не лучший вариант с точки зрения безопасности. Если вы отключите «Присоединиться перед хостом» внутри Настройки учетной записи Zoom, участники, которые входят в совещание, увидят на экране диалоговое окно «Собрание ожидает присоединения организатора» и смогут присоединиться к сеансу совещания только после того, как организатор войдет в сеанс.

НЕ позволяйте удаленным участникам повторно присоединяться



Zoom предлагает возможность разрешить участникам, которые ранее присутствовали на собрании, вернуться на собрание. Однако, если вы хотите, чтобы сеанс собрания был безопасным и защищенным, вы можете отключить параметр «Разрешить удаленным участникам присоединяться» в разделе «На собрании (базовый)» внутри Настройки учетной записи Zoom. Это предотвратит повторное участие ранее удаленных участников собрания и участников вебинара.