DOI 10.36622/VSTU.2022.25.3.005
УДК 004.056.55:003.26

ТЕХНОЛОГИИ ВИДЕОКОНФЕРЕНЦСВЯЗИ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, К.П. Колпаков

Рассматривается подход к обеспечению информационной безопасности в технологиях реализации видеоконференцсвязи и прочих технологиях медиакомунникаций. А также вопрос обеспечения безопасности при проведении видеоконференций и передаче данных как между двумя пользователями, так и групп пользователей. Рассматриваются типы ВКС и способы их реализаций, а также примеры программных решений, их возможностей и полного функционала. Подходы к созданию защищенного соединения канала передачи данных, а также базовые правила безопасности при организации и администрировании видеоконференций пользователей. В работе так же уделяется внимание развернутой политике сервисов по предоставлению услуг ВКС как для рядовых пользователей, так и для бюджетных и коммерческих организаций, отвечающих современным нормам информационной безопасности при проведении ВКС. Представлены, помимо традиционно рассматриваемых технических аспектов, вопросы обеспечения информационной безопасности с позиций организации проведения сессий, а также обеспечения режима конфиденциальности процессов ВКС.

Ключевые слова: видеоконференция, видеоконференцсвязь, ВКС, криптографическая защита, P2P, MP, stream, протокол, кодек, безопасность, виртуальный фон, администрирование, chromakey, медиакомуникации, функционал.

Видеоконференцсвязь

За сравнительно короткий период времени видеоконференцсвязь показала огромнейший скачок в развитии. На данный, момент видеоконференцсвязь (ВКС) – вершина современных медиакомуникаций, включающая в себя самые передовые сетевые решения: передачу высококачественного видео, голоса и данных.

В первую очередь ВКС используется для семинаров и дистанционного обучения. Большинство компаний интегрируют свою корпоративную связь в ВКС для того, чтобы снизить затраты на командирование сотрудников [1].

Именно благодаря современным средствам передачи данных и стремительному прогрессу в сфере информационных технологий, у людей появилась возможность организации реального социального взаимодействия в онлайн режиме, без угрозы жизни и здоровью, в виде, максимально приближенном к реальному общению (рис. 1).

Типы ВКС

Двухточечная («точка-точка», «point-to-point», «P2P») – два собеседника соединяются друг с другом напрямую. Это видеоаналог обычного телефонного соединения [2].

Многоточечная («многоточка», «multipoint», «MP») – в видеоконференции имеют возможность участвовать трое и более человек, которые могут собраться в виртуальном помещении для совещаний, находясь при этом за компьютером в офисе, дома или в дороге. Требуется сервер многоточечных видеоконференций [2].

Потоковая – подключение к видеоконференции других пользователей, которые могут наблюдать совещание на удаленном компьютере или мобильном устройстве, с помощью программных решений. Требуется сервер многоточечных видеоконференций и средства трансляции [2].

Рис. 1. Пример устройства переговорной комнаты с аппаратным решением ВКС

Примеры программных решений

1) **Zoom** – программа для видеоконференций, разработанная Zoom Video Communications. На данный момент она занимает ведущую позицию в выборе пользователей в разных сферах деятельности: удаленная работа, дистанционное обучение, вебинары, индивидуальное общение и т.п.

Zoom отличается простотой использования – для того, чтобы подключиться к видеоконференции достаточно скачать приложение и перейти по ссылке организатора. Также преимуществом является его доступность, возможность бесплатной организации видеоконференций с достаточно большим количеством участников (до 100 человек), которые свободно могу общаться друг с другом. Zoom использует шифрование на стороне клиента с использованием AES 256.

2) **TrueConf** – это сервер видеоконференцсвязи, разработанный российской компанией с одноименным названием. Архитектура программного обеспечения базируется также на российской разработке SVC. Также сервисом поддерживается интеграция со сторонними производителями по протоколам SIP и H.323. Платформу выбирают и одобряют государственные структуры, нуждающиеся в качественной и безопасной связи. Также сервер распространен в образовательной сфере и сфере финансов.

Возможности:

- Конференции с количеством участников до 1600 человек.
- Видеоконференции с разрешением до 4К и 60 к/с.
- Возможности проведения закрытых конференций и открытых вебинаров.
- Возможность подключения не авторизированных пользователей к вебинарам.
- Возможность вызова абонентов IP АТС.
- Возможность работы как с номерами стационарных, так и с номерами мобильных телефонов.
- Возможность передачи DTMF команд.
- Режимы видеосвязи: звонок один-на-один (точка-точка) и конференции трёх типов – все на экране, видеоурок и видеоселектор.
- Ведущий конференции – имеет возможность задать принудительно раскладки всем участникам, также может задать раскладки для каждого абонента

индивидуально, в том числе для SIP/H.323-терминалов и браузеров.

Поддерживаемые протоколы и кодеки:

Протоколы - собственный протокол TrueConf на базе технологии SVC, стандарт H.323, протоколы SIP, WebRTC, RTSP, Поддержка QoS, поддержка шифрования по ГОСТу, OAuth 2.0 [3].

Стандарты аудиосжатия - Opus, G.711, G.722, G.722.1, G.722.1C, G.723, G.728, G.729A, Speex, MP3, AAC.

Стандарты видеосжатия - VP8 SVC, VP8, H.264, H.264 AVC, H.264 SVC, X-H264UC, H.263, H.263+, H.263++

Основной функционал:

- Работа в закрытых сетях;
- Настройка качества записи видеоконференций;
- Возможность тонкой настройки HTTPS;
- Интеграция со сторонними ВКС-платформами;
- Передача данных между участниками конференции, минуя сервер;
- Трансляция конференций;
- Можно просматривать отчёты: о подключениях, о звонках, о сообщениях, о статусах, об устройствах пользователей.

Совместимость с операционными системами: совместим с Windows, macOS и Linux, android, IOS/iPadOS, Videobar, Kiosk, Room.

3) **Google Meet** – сервис видеоконфенренцсвязи от компании Google. Позволяет проводит конференции длительность до 60 минут, посредством браузера, либо одноименного приложения. В функционал включены стандартные функции – демонстрация экрана, интерактивная доска, и т.п. Используется стандарт WebRTC.

Поддерживается IOS/iPadOS, Windows, Chrome OS, Ubuntu и другие дистрибутивы Linux, android. Сервис отличается высокими требованиями для стабильной работы.

4) **Discord** – приложение, включающее в себя возможности текстового, голосового и видео - общения. Сервис пользуется популярностью среди геймеров, как платформа для онлайн-обучения, удаленной работы, личных видеоконференций и онлайн-мероприятий.

Приложение позволяет организовывать видеосвязь в приватном режиме, создавать публичные и приватны чаты и каналы, голосовые конференции, работать по принципу push-to-talk.

Используются следующие кодеки: для видео - VP8; для аудио - кодек Opus, обладающий возможностью эхоподавления и посторонних шумов, также обладает APУ.Имеется версия для браузера, также есть отдельное приложение [4].

5) **Skype** – ПО, позволяющее реализовывать обмен текстовой информацией, голосовой и видеосвязью, есть возможность передачи файлов и демонстрации экрана. Существует на рынке еще с 2003 года. На данный момент сервис не имеет отличительных особенностей,и по сравнению с другими, не отличается стабильным соединением. Поддерживается: Windows, Linux, macOS, iOS, Android, Windows Mobile, Windows Phone, PSP.

6) **Jitsi Meet** – бесплатное ПО для реализации видеоконференций на базе WebRTC, то есть в режиме браузера. ПО позволяет организовывать видеозвонки с количеством участников до 75. Обладает очень скудным функционалом. Подходит для личных видеозвонков и онлайн-образования. Поддерживается: Linux, Windows, macOS, iOS и Android.

7) **Microsoft Teams** – платформа, предназначенная для совместной работы в режиме видеозвонков и чатов. Позволяет производить обмен файлами, проводить демонстрации экрана, одновременную работу в режиме реального времени над редактированием и созданием документов, предоставляется облачное хранилище. Является платной, так как включена в пакет Office 365. Нет совместимости с другими сервисами ВКС. Используется в пределах компаний и организаций, которые активно используют Office 365.

8) **Slack** – чисто корпоративный мессенджер, включающий в себя большое количество возможностей, одной из которых является реализация видеоконференций. Используется многими медиаизданиями и IT-

компаниями (eBay, Pikabu, PayPal, Adobe). Поддерживается: Linux, Windows, macOS, iOS и Android

9) **GoToMeeting** – приложение для веб-конференций, включающее стандартный функционал: демонстрацию экрана, совместную работу над документами, запись видеоконференций и т.п. Отличается высоким уровнем безопасности личных данных пользователей.

10) **Яндекс Телемост –** отечественный онлайн-сервис для организации и администрировании видеозвонков. Время вызова между пользователями неограниченно, в конференции могут состоять вплоть до 40 участников. Функционал достаточно невелик: возможность включения и выключения микрофона, камеры, также есть возможность делится экраном. На данный момент поддерживаемые операционные системы: Windows, Linux. Загвоздка состоит в том, что в настоящее время осуществлять видеозвонки можно только в «Яндекс Браузер», Google Chrome и Mozilla Firefox с персонального компьютера.

Отечественная система ВКС - TrueConf Server

TrueConf Server это отечественная система ВКС на базе архитектуры SVC (рис. 2). Каждый из участников видеоконференции получает от сервера видео оптимального качества, которое поддерживает конкретные устройства и каналы связи (рис. 3). Использование отечественных платформ ВКС становится особенно актуальным прежде всего, исходя требований обеспечения информационной безопасности при организации ВКС, для надежного обеспечения защиты информации, в случаях, когда в процессе совещаний может использоваться информация ограниченного доступа, сведения конфиденциального характера. Значимость отечественных систем ВКС усугубляется в рамках реализации эффективной политики импортозамещения.

Безопасность

Вопросы обеспечения безопасности при проведении видеоконференций и передаче данных на сегодняшний день стоят особенно остро, поскольку вместе с развитием технологий прогрессирует и рост утечек данных, что неприемлемо не только для глобальных компаний, но и для рядовых пользователей. Для решения этих проблем разработаны и активно используются комплексы криптографической защиты данных – решение для компаний. Для обычных пользователей актуально соблюдение базовых правил безопасности в сети:

- Уникальный и надежный пароль;
- Многофакторная аутентификация;
- Загрузка приложений из официальных источников;
- Корректировка настроек конфиденциальности ПО;
- Своевременное обновление ПО, которое используется для проведения ВКС;
- Проведение видеоконференции по уникальному идентификатору;
- Переход только по проверенным ссылкам от доверенных лиц;
- Получать, скачивать и открывать документы только от доверенных лиц;
- Устанавливать в настройках конференции допуск участников только с разрешения модератора конференции;
- Доступ к записи видеоконференции следует ограничивать.

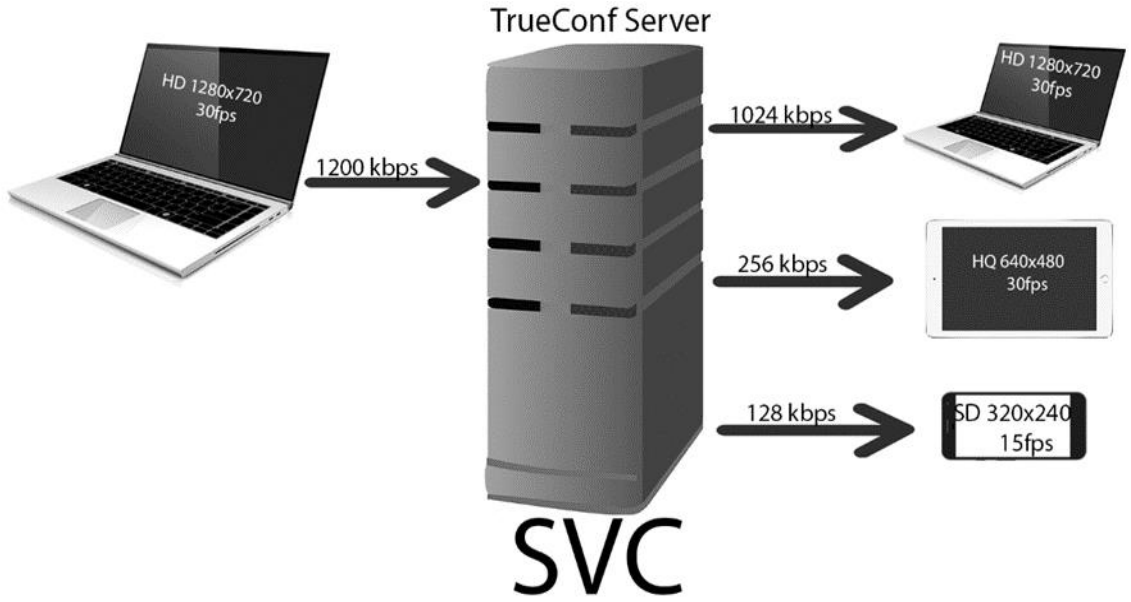

Рис. 2. TrueConf Server

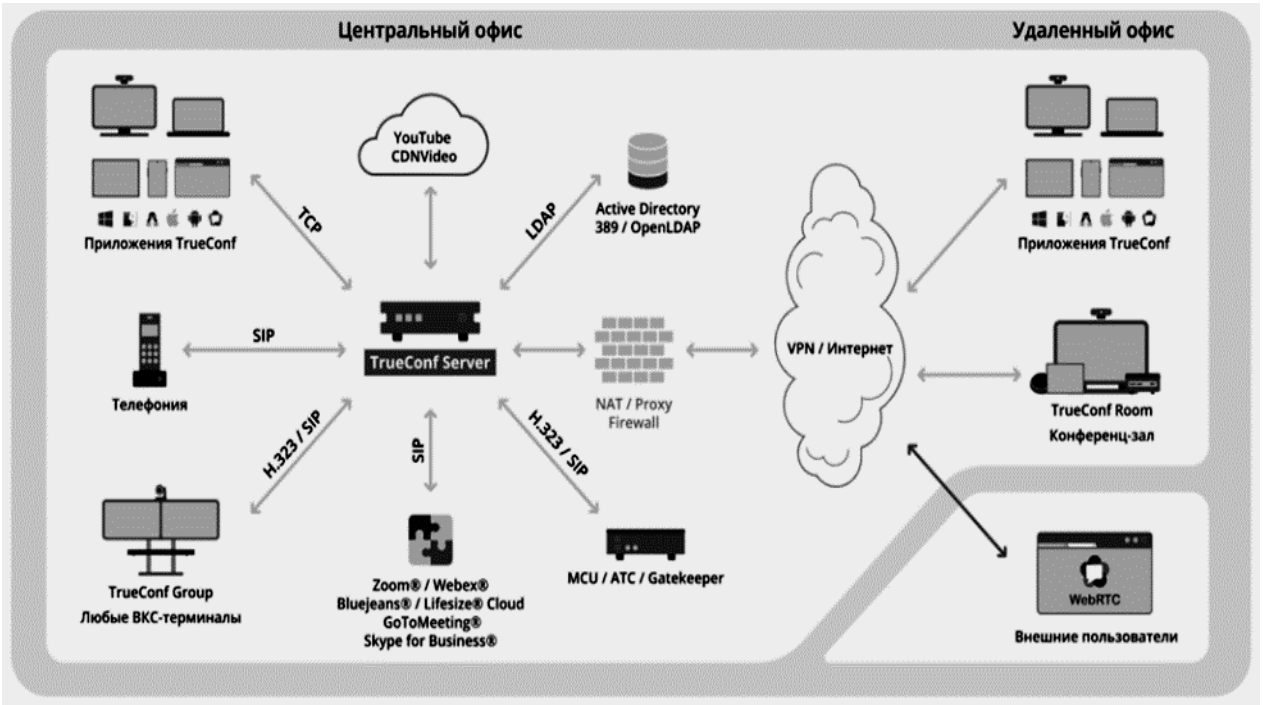

Рис. 3. TrueConf Server

Как злоумышленники могут получить ваши личные данные:

1. Клон оригинального приложения. Злоумышленники полностью копируют оригинальный сайт, покупают доменное имя максимально похожее на оригинальный сайт. Например, сайт компании zoom имеет такое имя – «zoom.us», злоумышленники называют сайт z00m.us используя вместо двух букв «о»

два нуля. У рядового пользователя это вполне не вызовет никаких подозрений. При помощи рекламы и продвижения сайтов они поднимают свой сайт на первые места выдачи результата по поиску пользователя.

Компания Яндекс стала верифицировать сайты и выдавать оригинальным сайтам галочку. Это является одним из способов борьбы с мошенниками (рис. 4).

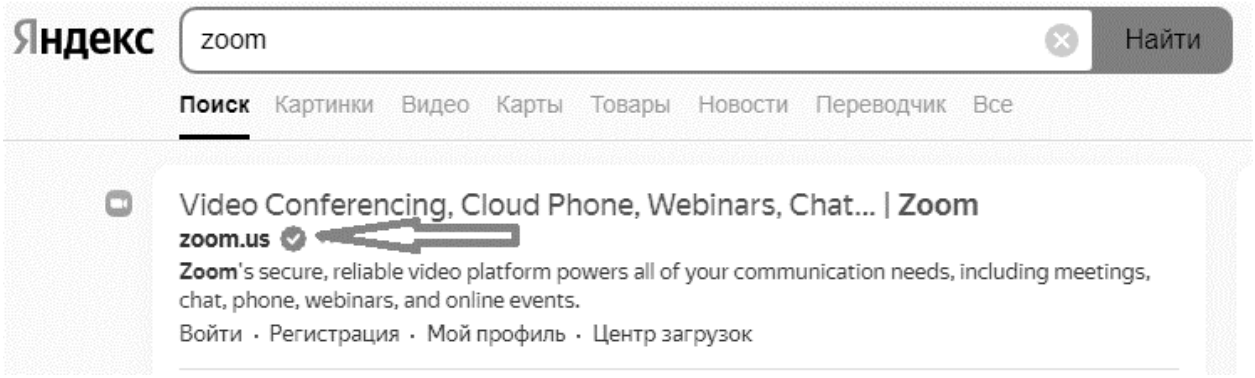

Рис. 4. Пример идентификации оригинального сайта

Часто инсталляторы можно найти и на сторонних сайтах: загрузив их и установив, пользователь скорее всего увидит всплывшее окно с предупреждением о том, что устанавливаемая программа из неизвестного источника и что ее установка является опасной и нежелательной. Большинство пользователей игнорируют это. Установив программу, пользователь видит полностью скопированное с оригинала приложение, с ничем не отличающимся дизайном и интерфейсом. Вводя свои данные он почти что добровольно передает их в руки злоумышленников, а в худшем случае заразит ПК или же мобильное устройство программой шпионом или же классическим трояном. А что если это корпоративное устройство? В таком случае злоумышленник сможет проникнуть в корпоративную сеть и иметь доступ к информации компании, манипулировать ей, а также получить доступ к коммерческой тайне и иной конфиденциальной информации.

Также клоны приложений могут предоставить вам возможность регистрации на данном ресурсе: жертва заполняет форму регистрации, вводит свои личные данные, такие как ФИО, электронную почту, номер мобильного телефона и даже место жительства. Злоумышленник может получить доступ к камере или микрофону, вести слежку за жертвой. Всю полученную информацию преступник может продавать, обнародовать или же использовать в иных целях.

Так, о некоторых уязвимостях системы безопасности в Zoom уже сообщалось ранее. В 2019 году было обнаружено, что приложение Zoom устанавливало на устройства пользователей скрытый веб-сервер, с помощью которого пользователя можно было принудительно добавить в видеочат.

2. Утечки при недобросовестном составлении данных для входа в систему. Пользователи не задумываются о частой смене паролей, или же используют один и тот же пароль в огромном количестве сервисов. Не редко на слуху появляются новости об обнародовании огромных баз с паролями пользователей. Приведем пример недавней утечки огромной базы паролей. Речь идет о немыслимом количестве данных, а именно более 8 млрд паролей, огромное количество из них является простыми. Эксперты предполагают, что эти пароли — компиляция предыдущих утечек. Логинов в файле нет, только пароли размером от 6 до 20 символов. Огромное их количество — сложные пароли со спецсимволами. Все они содержатся в одном файле с названием RockYou2021.txt.

Существуют огромные базы личных данных, которые утекают в сеть по тем или

иным причинам. Злоумышленнику не составит больших проблем методом подбора попробовать получить доступ к вашей учетной записи и использовать это в своих интересах.

По информации на 2020 год в России количество утечек персональных данных, а также логинов и паролей в сеть возросло на треть. Примерно 100 миллионов записей персональных данных граждан. Большая часть - примерно 70% - пришлась на сотрудников компаний.

Использование простых и одинаковых комбинаций паролей ставит под угрозу пользователей ВКС и не только их.

3. Утечка данных при демонстрация излишнего количества информации. Большинство сервисов предлагают функцию демонстрации экрана, но ни в коем случае нельзя демонстрировать больше данных, чем нужно в данном конкретном случае. Показывать документы, имена файлов и вкладки браузера. Необходимо контролировать список участников конференции, вести надзор за подключениями новых пользователей в конференцию, чтобы не допускать посторонних к сеансу. Человек, имеющий права администратора конференции, должен настроить сервис правильно, так чтобы участникам не было разрешено ничего лишнего, присутствовал контроль за количеством вступивших и за тем, кто вообще вступает в конференцию.

Также при регистрации и создании совей учетной записи не стоит указывать слишком много информации о себе, своей семье, выкладывать фото и видео, которые могут скомпрометировать и быть использованы против вас. Информация, которую вы указываете о себе, должна быть краткой, малоинформативной (рис. 5). Кроме того, отдельно предусматривается «Раздел» или «Пункт» «Безопасность» (рис. 6).

4. Уязвимости используемых сервисов.

В данном пункте хотелось бы описать то, что не все приложения, которые имеют высокий рейтинг и большое количество пользователей, отвечают всем требованиям информационной безопасности. Как и везде, тут тоже не обходится без изъянов в самой структуре приложения или в его шифровании. Причиной тому может быть экономия средств, некомпетентность команды, которая над ним работала, прекращение отслеживания ошибок после запуска приложения, приостановка выпуска новых патчей, элементарные ошибки при написании программы – все это также ставит ваши данные под большую угрозу.

Так, например, за последнее время в приложениях Zoom обнаружили целый букет уязвимостей разной степени значимости: в клиентах для Windows и macOS нашелся баг, позволяющий похитить учетные данные от компьютера. Еще два бага в приложении для macOS могли стать причиной полного захвата устройства.

Помимо этого, стоит отметить то, что некоторые разработчики изначально создают свои приложения с целью хищения данных и последующего их использования, не применяя никакого шифрования, оставляя огромные бреши в защите приложения.

Поэтому любой пользователь должен быть бдительным, должен внимательно выбирать то, чем он будет пользоваться, куда он вводит свои данные и на что соглашается. Необходимо изучать отзывы из независимых источников, следить за сводками новостей в разделе информационной безопасности.

5. Неправильная настройка конференции или же ее отсутствие.

Перед тем, как создавать конференцию и приглашать в нее пользователей, администратор должен провести настройки, соответствующие потребностям будущего сеанса, во избежание подключения сторонних пользователей, и пользователей, которые имеют корыстный интерес. Самым надежным способом считается защита конференции паролем. И еще один из способов — это включение комнаты ожидания. Суть заключается в том, что желающие присоединиться к видеоконференции попадают в «лист ожидания» и остаются в нем, пока администратор не одобрит их участие.

И тут стоит быть максимально внимательным, поскольку пароль может уйти от приглашенных участников, или же кто-то

решит устроить глупую шутку. В вопросе кибербезопасности следует быть и оставаться максимально бдительным, ведь от этого зависит ваша приватность в сети.

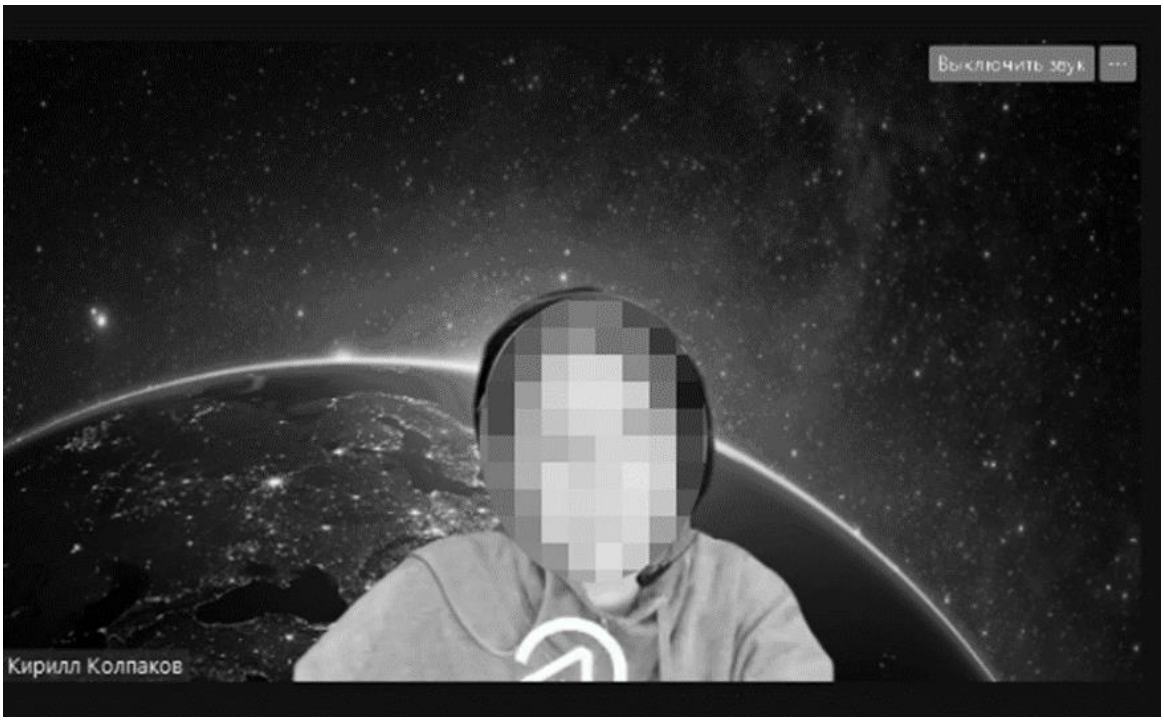

Рис. 5. Применение виртуального фона в конференции

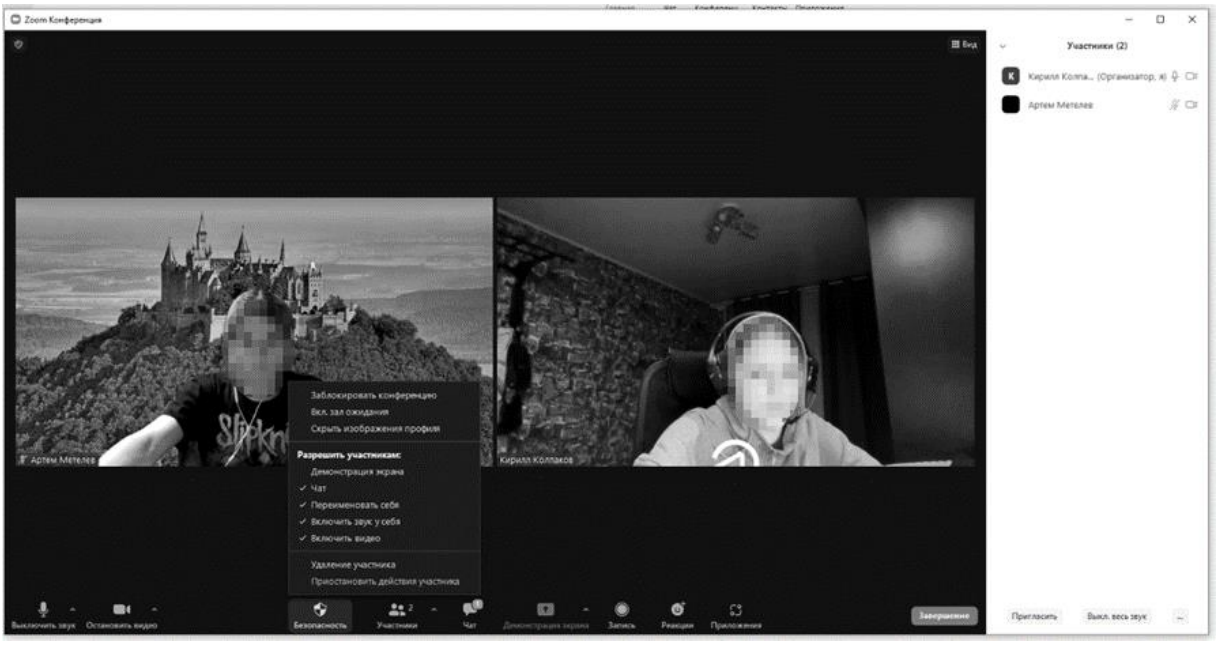

Рис. 6. Пункт безопасность

Комплексы криптографической защиты данных обычно устанавливаются на входе локальной сети. Они осуществляют шифрование и дешифрование информации внутри локальной сети компании, создавая безопасное пространство для коммуникации, ограничивая анализ трафика, сохраняя

конфиденциальность оборота данных и их целостность.

Пункт «Безопасность» - предоставляет возможности блокирования конференции, в случае какой-то угрозы и т.п., возможность включения зала ожидания, также скрытие фото профиля своего и участников (рис. 6).

Также, для обеспечения безопасности служит пункт «Управления участниками в целом». Он позволяет участникам включать демонстрацию своего экрана, общаться и писать в чате, самим переименовывать себя, включать и выключать свои микрофон и камеру. Можно удалить участника и приостановить любые его действия.

Пункт «Настройки виртуального фона». По ходу конференции и перед ней есть возможность изменить свой виртуальный фон без возможности использования хромакея. При этом нужно соблюдать ряд условий, чтобы фон четко и конкретно занял свое соответствующее положение (рис. 6).

Вообще для чего нужен виртуальный фон? В первую очередь, он используется для скрытия отвлекающих факторов как для всех участников конференции, так и для выступающего. Во-вторых, это позволяет перекрыть окружающую вас обстановку (создание личного пространства, исключение демонстрации личной жизни).

В распоряжении имеются три варианта:

- размытие фона (фокус направлен на докладчика, фон размыт);
- выбор изображения для фона самостоятельно (из своей галереи и т.п.);
- или же выбор изображения из предустановленных в ПО.

Для использования данной возможности в полной мере необходимо соблюдать ряд правил:

- хорошее освещение напротив вас;
- стоит подбирать одежду, не совпадающую с предлагаемыми вам фонами, или заранее выбранным вами фоном;
- стоит расположиться напротив стены (то есть статичного, желательно, однотонного объекта).

Список литературы

1. Видеоконференцсвязь. Что такое видеоконференцсвязь? URL: https://www.aitek-d.ru/videokonferencsvyaz.html (дата обращения: 3.08.2022).

2. Технологии видеоконференцсвязи. URL: http://www.portal-yug.ru/services/integration/services/videoconference/ (дата обращения: 3.08.2022).

3. Протокол H.323/SIP. URL: https://support.zoom.us/hc/ru/categories/200110033 (дата обращения: 3.08.2022).

4. Кодеки, использующиеся в видеоконференциях:URL: https://trueconf.ru/blog/baza-znaniy/kakie-audiokodeki-ispolzuyutsya-v-po-trueconf.html (дата обращения: 3.08.2022).

Московский государственный лингвистический университет
Moscow State Linguistic University

Сыктывкарский государственный университет им. Питирима Сорокина
Syktyvkar State University after the Pitirim Sorokin

Поступила в редакцию 04.08.2022

Информация об авторах

Филяк Петр Юрьевич – канд. техн. наук, директор Института информационных наук Московского государственного лингвистического университета, e-mail: p,filiak@linguanet.ru

Колпаков Кирилл Николавевич – студент бакалавриата направления подготовки «Информационная безопасность», Сыктывкарский государственный университет, e-mail: zadose442094@yandex.ru

VIDEOCONFERENCING TECHNOLOGIES AND INFORMATION SECURITY

P.Yu. Filyak, K.P. Kolpakov

An approach to ensuring information security in video conferencing and other media communication technologies is considered. As well as the issue of ensuring security during videoconferences and data transmission between two users and groups of users. The types of VCS and methods of their implementations are considered, as well as examples of software solutions, their capabilities and full functionality. Approaches to creating a secure data link connection, as well as basic security rules for organizing and administering user video conferences. The work also pays attention to the detailed policy of services for the provision of VCS services for both ordinary users and for commercial and budgetary institutions that meet modern information security standards when conducting VCS. In addition to the traditionally considered technical aspects, the issues of ensuring information security from the standpoint of organizing sessions, as well as ensuring the confidentiality of VCS processes, are presented.

Keywords: Videoconferencing, videoconferencing, videoconferencing, cryptographic protection, P2P, MP, stream, protocol, codec, security, virtual background, administration, chomakeu, media communications, functionality.

Submitted 04.08.2022

Information about the authors

Petr Yu. Filyak – Dr. Sc. (Technical), Director of the Institute information Sciences, Moscow State Linguistic University, e-mail: p.filiak@linguanet.ru

Kirill P. Kolpakov – Bachelor of Information Security, Syktyvkar State University, e-mail: zadose442094@yandex.ru