

60. ВИДЕОКОНФЕРЕНЦСВЯЗЬ И ОБЕСПЕЧЕНИЕ ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кожемякина М.В., студент гр.478104, Федюкович Т.В., ассистент кафедры ЭИ

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь,*

Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ

Аннотация. Статья анализирует современные подходы к обеспечению безопасности видеоконференцсвязи в условиях активного развития удаленной работы и онлайн-обучения. Рассмотрены основные угрозы информационной безопасности. Особое внимание уделено практическим рекомендациям по защите конфиденциальных данных. Подчеркивается необходимость повышения осведомленности пользователей о потенциальных рисках и обучении их безопасному поведению во время видеоконференций.

Ключевые слова: видеоконференцсвязь, видеоконференция, информационная безопасность, защита данных, атаки, конфиденциальность, угрозы, удаленная работа, аутентификация, шифрование.

В условиях стремительного развития информационных технологий и глобализации коммуникаций особо актуальными становятся инструменты, позволяющие обеспечивать эффективное взаимодействие между людьми на расстоянии. Одним из таких инструментов является

видеоконференция — технология, объединяющая аудио- и видеосвязь для проведения встреч в режиме реального времени.

Видеоконференция — это сеанс связи между двумя пользователями или группой пользователей, независимо от их месторасположения.

Видеоконференцсвязь (ВКС) стала неотъемлемой частью современной деловой и социальной коммуникации, особенно в условиях роста удалённой работы и онлайн-обучения.

ВКС основана на передаче данных через интернет или специализированные сети. Для её реализации используются камеры, микрофоны, динамики и программное обеспечение, обеспечивающее кодирование и декодирование сигналов. Современные платформы, такие как Zoom, Discord, Microsoft Teams и Google Meet, предоставляют удобный интерфейс для проведения видеоконференций с возможностью демонстрации экрана, записи встреч и совместного редактирования документов.

Основным преимуществом ВКС является минимизирование географических ограничений. Участники могут находиться в разных уголках мира, но при этом взаимодействовать визуально и аудиально. Это особенно важно для международных компаний, которые стремятся снизить затраты на командировки, а также для образовательных учреждений, занимающихся онлайн-обучением студентов. Кроме того, видеоконференцсвязь способствует повышению продуктивности за счёт экономии времени и улучшению качества коммуникации благодаря визуальному контакту [1].

Однако внедрение ВКС сопряжено с рядом сложностей. К ним относятся необходимость высокоскоростного интернет-соединения и вопросы конфиденциальности участников видеоконференций. Во многих странах действуют строгие законы о защите данных, такие как Общий регламент по защите данных (GDPR) в Европейском союзе или Закон Республики Беларусь №99-3 от 7 мая 2021 года «О защите персональных данных». Эти нормативные акты требуют, чтобы организаторы видеоконференций обеспечивали безопасность данных участников, включая видео-, аудиоинформацию и текстовые сообщения в чате.

Вот несколько примеров атак на пользователей систем видеоконференцсвязи, которые могут совершать злоумышленники:

Незванные участники: в этом случае посторонний человек проникает на видеовстречу с целью подслушать разговор или нарушить ход мероприятия, распространив неприемлемый контент.

Опасные ссылки в чате: злоумышленники, получив доступ к конференции, могут делиться вредоносными ссылками через чат. Переход по таким ссылкам может привести к краже личных данных или установке вредоносного программного обеспечения.

Использование украденных ссылок: если одна и та же ссылка используется для нескольких встреч, это упрощает задачу злоумышленникам, которые могут воспользоваться ей для несанкционированного доступа.

Захват роли организатора: при такой атаке участник дожидается момента, когда организатор конференции покидает встречу раньше остальных, чтобы занять его место и получить контроль над видеовстречей.

Согласно общепринятой классификации, угрозы информационной безопасности подразделяются на три основные категории: нарушение целостности данных, утечка конфиденциальной информации и проблемы с доступом к ресурсам [2]. Все эти типы угроз в той или иной степени применимы к видеоконференциям. Например, когда количество желающих подключиться к открытой конференции превышает возможности канала связи, главной задачей становится обеспечение бесперебойного доступа для всех участников. Для решения этой проблемы можно использовать технологии распределения сетевой нагрузки. Чтобы защитить данные от искажений или потерь, рекомендуется применять помехоустойчивое кодирование. Для проведения конфиденциальных видеоконференций важно ограничить доступ для незарегистрированных пользователей, а также внедрить механизмы идентификации устройств и проверки подлинности участников.

Как и любая другая информационная система, системы видеоконференцсвязи сталкиваются с различными угрозами. Это могут быть, к примеру, атаки злоумышленников и ошибки, допущенные пользователями или администраторами. Вопросы защиты таких систем особенно важны в современных условиях, поскольку онлайн-обучение и удаленная работа становятся всё более востребованными благодаря доступности из любой точки мира. В то же время организаторы видеоконференций предъявляют всё более высокие требования к качеству сервиса и надежности связи.

Ниже представлен список ключевых рекомендаций, которых стоит придерживаться участникам видеоконференций. Однако не все из них могут быть выполнимы при использовании конкретного программного обеспечения видеосвязи:

При планировании новой встречи рекомендуется использовать функцию регистрации участников. Многие платформы предоставляют такую возможность, позволяя проводить собрания,

доступные только зарегистрированным пользователям. Это обеспечивает подключение лишь авторизованных лиц через защищенные ссылки, без необходимости ввода дополнительного пароля.

Аутентификация участников: многие платформы поддерживают двухфакторную (2FA) или многофакторную (MFA) аутентификацию либо напрямую, либо через интеграцию с внешними сервисами идентификации (например, Okta, Azure AD и другими). Если по каким-либо причинам невозможно использовать двухфакторную или многофакторную аутентификацию, необходимо придерживаться нижеперечисленных правил.

Следует создавать уникальные пароли для каждой встречи: убедитесь, что каждый сеанс видеоконференции защищен отдельным паролем. Ни в коем случае не делайте пароли общедоступными.

Следует избегать использования личных комнат: для каждой встречи создавайте уникальный идентификатор. Причина в том, что личные комнаты обычно имеют постоянную ссылку, и любой, кто знает этот адрес, может без труда присоединиться к конференции.

Лучше использовать функцию комнаты ожидания: она размещает участников в отдельное виртуальное пространство до начала собрания, позволяя организатору контролировать, кто именно будет допущен к участию.

Нужно включить оповещение о входе участников: система будет подавать звуковой сигнал при подключении каждого нового участника. Это позволит всем, даже тем, кто участвует только через аудио, понять, кто присоединился, и при необходимости запросить у нового участника дополнительную информацию.

Следует применять современные методы шифрования: проверенные алгоритмы, такие как AES, и отдавайте предпочтение более длинным ключам, которые обеспечивают повышенный уровень защиты (например, 256-битный ключ безопаснее, чем 128-битный, а 4096-битный надежнее, чем 2048-битный).

Нужно использовать сквозное шифрование (End-to-End, E2E): при таком подходе только участники конференции смогут видеть и слышать происходящее, так как данные защищены на всем пути передачи — от отправителя до получателя. Если же сквозное шифрование не используется, третьи стороны, например, провайдеры видеоконференцсвязи, могут получить доступ к информации, особенно если это потребуется по закону или из-за внутренней политики компании. Без E2E конфиденциальность данных полностью зависит от того, насколько надежно их защищает провайдер. Однако не все встречи требуют использования сквозного шифрования (E2E). Необходимость в нем определяется спецификой деятельности и темой собрания. Например, открытый онлайн-урок по физкультуре вряд ли нуждается в таком уровне защиты, тогда как обсуждение конфиденциальных вопросов корпоративной стратегии требует повышенной безопасности.

Следует заблокировать доступ для новых лиц: после того как все участники присоединились к конференции, заблокировать доступ, чтобы предотвратить присоединение посторонних лиц.

Целесообразно удалять неизвестных или нежелательных участников: если на встречу проник кто-то посторонний или участник ведет себя некорректно, его можно исключить из конференции. Также можно активировать настройки, которые предотвратят возможность повторного подключения таких участников.

Включать видео следует только при необходимости: отключение камеры и использование только аудио помогает защитить конфиденциальность участников, так как злоумышленники могут использовать детали обстановки для сбора информации о них. Кроме того, отказ от видео снижает нагрузку на сетевое соединение, что положительно сказывается на качестве звука и изображения во время собрания.

Необходимо с осторожностью использовать чаты: все обмены сообщениями во время видеоконференций могут быть потенциально опасными, так как любой участник может распространить ссылку, содержащую неприемлемый контент. Особенно опасными являются приватные чаты (между двумя участниками видеоконференции), поскольку они происходят без ведома других. В случае если использование чата необходимо, настройте его таким образом, чтобы только организатор мог общаться с участниками, а участники не могли обмениваться сообщениями друг с другом и использовать приватный чат.

Нужно контролировать передаваемую информацию: участникам конференции следует внимательно следить за тем, чтобы случайно не поделиться конфиденциальной информацией во время видеозвонка. Рекомендуется предоставлять доступ только к определенным приложениям, избегая демонстрации всего рабочего стола.

Следует запретить обмен файлами: отключить функцию передачи файлов, чтобы предотвратить возможность обмена нежелательным контентом во время видеоконференции.

Лучше сохранять записи только важных встреч: если запись не является необходимой, предпочтительнее обойтись без нее.

Надо применять подходящий уровень аутентификации и шифрования: выбор уровня защиты зависит от специфики конкретной встречи. Некоторые конференции могут быть предназначены для широкой аудитории и транслироваться на платформах вроде YouTube, тогда как другие должны быть доступны только ограниченному кругу участников.

Необходимо использовать защищенные устройства: лучше подключаться к видеоконференциям только с устройств, защищенных антивирусным программным обеспечением и брандмауэром.

Следует выбирать надежные провайдеры ВКС: использовать платформы, которые соответствуют международным стандартам безопасности (например, ISO 27001) и предоставляют подробную информацию о своих методах защиты данных [3].

Лучше минимизировать использование общедоступных сетей: избегать подключения к видеоконференциям через публичный Wi-Fi. Предпочтительнее использовать защищенное VPN-подключение.

Сегодня видеоконференции являются основным инструментом для делового взаимодействия как внутри компаний, так и за их пределами. Популярность платформ видеоконференцсвязи продолжает расти, охватывая все больше пользователей по всему миру. Однако широкое распространение этой технологии привлекло внимание злоумышленников, которые могут заниматься как распространением неприемлемого контента, так и целенаправленным шпионажем. Поэтому важно предоставлять компаниям и сотрудникам, работающим удаленно, рассмотренные в статье рекомендации для обеспечения безопасности видеоконференций и защиты конфиденциальных данных пользователей.

В статье были проанализированы способы обеспечения безопасности видеоконференцсвязи. Были рассмотрены основные угрозы информационной безопасности, такие как незванные участники, опасные ссылки в чате, использование украденных ссылок и захват роли организатора. Проведён анализ ключевых рекомендаций по защите видеоконференций, включая использование функции регистрации участников, двухфакторной аутентификации, сквозного шифрования (E2E), блокировки доступа для новых лиц, создание уникального пароля для каждой видеоконференции и минимизирование использования общедоступных сетей. Каждая из рекомендаций имеет свои преимущества и ограничения, однако их применимость зависит от специфики конкретной встречи и используемого программного обеспечения для ВКС.

Статья знакомит со способами минимизации рисков при проведении видеоконференций, при этом подчеркивается важность сочетания технического и организационного подходов. Ввиду ограничений отдельных методов защиты, таких как зависимость от качества интернет-соединения или уровня шифрования, ни один из способов не является универсальным решением. Поэтому наиболее эффективным является использование комплексного подхода, который сочетает в себе как технические меры защиты, так и организационные — обучение пользователей безопасному поведению во время видеоконференций.

Список использованных источников:

1. Сороцкий В. А., Цикин И. А. *Современные системы видеоконференцсвязи: учебное пособие*. – Санкт-Петербург: Издательство Политехнического университета, 2010.
2. Нестеров С. А. *Информационная безопасность: учебник и практикум для академического бакалавриата*. – Москва: Издательство Юрайт, 2019.
3. Родичев Ю. А. *Нормативная база и стандарты в области информационной безопасности: учебное пособие*. – Санкт-Петербург: Питер, 2017.

UDC 004.056.5