

УДК 621.391

ВЫБОР ПЛАТФОРМЫ ВИДЕОКОНФЕРЕНЦСВЯЗИ ДЛЯ УЧЕБНОГО ПРОЦЕССА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ПАРАМЕТРОВ

Довгулевич Е.В., магистрант гр.267041

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

Шевчук О.Г. – канд. техн. наук, доцент

Аннотация. В данном тезисе проведен сравнительный анализ основных параметров платформ видеоконференцсвязи для учебного процесса.

Ключевые слова. Видеоконференцсвязь, облачные сервисы видеоконференцсвязи, параметры видеоконференцсвязи.

Сегодня видеоконференцсвязь является неотъемлемой частью многих организаций, в том числе и учебных учреждений. Одним из ключевых инструментов онлайн-обучения является платформа видеоконференцсвязи, при выборе которой необходимо учитывать множество факторов, таких как функциональность, качество передачи видео и голоса, надежность, безопасность, совместимость программного обеспечения, удобство использования, стоимость. В данном тезисе будет проведен сравнительный анализ основных параметров платформ видеоконференцсвязи для учебного процесса.

В первую очередь следует определить параметры, по которым далее будем анализировать программные продукты. Поскольку рассматривать в рамках одних и тех же критериев облачных сервисов (cloud-based) и локальных (on-premise) некорректно, то для сравнения возьмем исключительно облачные решения. Они на текущий момент предоставляют наиболее широкий функционал и, кроме того, не требуют от организации аппаратных ресурсов для развертывания, а значит соотношение скорости их внедрения и необходимых для этого усилий наиболее оптимально [1]. Среди сервисов видеоконференцсвязи, которые широко используются в образовании, можно отметить Zoom, Microsoft Teams, Google Meet, Cisco Webex, Skype.

Первым критерием для сравнения является функциональность платформы. При выборе системы видеоконференцсвязи необходимо убедиться, что она поддерживает все необходимые функции. Возможность проведения онлайн-занятий и осуществление обменом файлов поддерживают все перечисленные сервисы видеоконференцсвязи. Важной функцией для студентов, которые не могут посещать занятия в режиме реального времени является возможность записи занятий, предоставляемая всеми указанными выше платформами. Проведение параллельных занятий для разных групп, управление доступом студентов к материалам и занятиям, возможность подключения большого количества участников позволяют сервисы видеоконференцсвязи Zoom, Microsoft Teams и Cisco Webex. Исходя из вышеперечисленных функций, можно сделать вывод, что все платформы имеют схожие базовые функции.

Вторым критерием является качество передачи видео и голоса, обусловливаемое различными факторами, такими как пропускная способность канала связи и использование кодеков. Системы конференцсвязи Cisco Webex и Microsoft Teams, поддерживают передачу видео и голоса высокого качества даже при низкой пропускной способности канала связи. Google Meet и Zoom имеют оптимизацию видео и аудио потоков в зависимости от качества канала связи на стороне конечного пользователя. В целом, все системы конференцсвязи стремятся обеспечить максимальное качество передачи данных при использовании доступных ресурсов.

Важным параметром при выборе платформы видеоконференцсвязи является обеспечение информационной безопасности, в части касающейся защиты от перехвата данных, управления доступом и хранения пользовательской информации [2]. Анализ безопасности программ для видеоконференций обозначил следующие важные моменты, на которые необходимо обращать внимание при выборе системы – это наличие сквозного шифрования, защиты от несанкционированного доступа, наличие двухфакторной аутентификации и количество уязвимостей.

Все сервисы видеоконференцсвязи придерживаются высоких стандартов безопасности. Каждый сервис имеет свои преимущества и недостатки, и лучше всего выбирать, основываясь на потребности и требования организации. Для удобства основные параметры, касающиеся безопасности приложений для видеоконференций представлены в таблице 1.

Проанализировав базу данных MITRE по уязвимостям в ПО (CVE - Common Vulnerabilities and Exposures) за 2021-2022 годы было обнаружено, что в приложениях Zoom, Microsoft Teams было зарегистрировано не менее 5 уязвимостей за этот период, Cisco Webex не менее 4 уязвимостей. Это демонстрирует, что в приложениях были обнаружены некоторые уязвимости, которые могут повлиять на безопасность пользователей. Однако обычно компании выпускают исправления на такие уязвимости в своих обновлениях. В Google Meet не зарегистрировано уязвимостей за этот период. Но это не гарантирует, что таких уязвимостей не было, потому что не все уязвимости, возникающие в ПО, могут быть зарегистрированы в базе данных MITRE [3].

Таблица 1 – Основные параметры, касающиеся безопасности приложений для видеоконференций.

Приложения	Zoom	Microsoft Teams	Cisco Webex	Google Meet
Основные параметры				
Шифрование данных	AES 256-битное шифрование	AES 256-битное шифрование	TLS 1.2/AES 256-битное шифрование	TLS и SRTP
Двухфакторная аутентификация	есть	есть	есть	есть
Возможность управления персональными данными на сервере	нет	есть	нет	нет
Возможность управления персональными данными на стороне клиента	есть	есть	есть	есть
Наличие комнаты ожидания	есть	есть	есть	есть
Соответствие стандартам безопасности	HIPAA, GDPR, FEBRA, SOC 2, ISO 27001	HIPAA, ISO 27001, SOC 1 и SOC 2	SOC 2, ISO 27001, HIPAA, PCI DSS и GDPR	SOC 2, ISO 27001 и HIPAA

В заключение, проведенный сравнительный анализ основных параметров видеоконференцсвязи для учебного процесса позволяет сделать вывод о том, что выбор платформы должен основываться на ряде факторов, включая доступность функциональных возможностей, а также безопасность и конфиденциальность данных. Необходимо учитывать, что каждая платформа имеет свои достоинства и недостатки, и выбор должен быть обоснованным и основываться на конкретных требованиях и задачах. Также, стоит учитывать, что технологии видеоконференцсвязи продолжают развиваться и улучшаться, поэтому важно следить за новыми тенденциями и обновлениями, чтобы выбирать наиболее подходящие решения для эффективной организации учебного процесса.

Список использованных источников:

1. ВКС для корпоративного использования: что выбрать и как сравнить? [Электронный ресурс]. Режим доступа: <https://slddigital.com/article/vks-dlya-korporativnogo-ispolzovaniya-cto-vybrat-i-kak-sravnit/>. Дата доступа: 05.04.2023.
2. Сравнение сервисов видеоконференций с точки зрения их безопасности. [Электронный ресурс]. Режим доступа: <https://www.anti-malware.ru/compare/Video-conferencing-software-security>. Дата доступа: 10.04.2023.
3. Search CVE List. [Электронный ресурс]. https://cve.mitre.org/cve/search_cve_list.html. Дата доступа: 03.04.2023.