КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.113122
УДК 004.056.5

Шабатура Марія Миколаївна
к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID 0000-0003-0814-1855
mariia.m.mandrona@lpnu.ua

Тихолаз Дмитрій Олександрович
Студент спеціальності «Кібербезпека»
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID 0000-0003-1014-5601
dtykholaz@email.com

Бумба Ірина Юріївна
Студентка спеціальності «Кібербезпека»
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID /0000-0002-1983-7260
bumba.iryna.2002@gmail.com

ДОСЛІДЖЕННЯ СТАНУ КІБЕРБЕЗПЕКИ СЕРВІСІВ ВІДЕОЗВ'ЯЗКУ

Анотація. Сервіси для онлайн зустрічей це чудові ресурси, які зараз, у час пандемії, рятують весь світ. Це ключовий компонент того, скільки підприємств продовжує функціонувати, університети, коледжі та школи можуть продовжувати викладати, а також те, як сім'ї та друзі можуть залишатися на зв'язку під час ізоляції. Відео-конференц-зв'язок це телекомунікаційна технологія інтерактивної взаємодії трьох і більше віддалених користувачі, при якій між ними можливий обмін аудіо- і відеоінформацією в реальному часі, з урахуванням передачі керуючих даних. На сьогоднішній день є чимало таких ресурсів, проте виникає питання «кому довіряти», адже у новинах часто зустрічається інформація про витік інформації через виявленні вразливості тих чи інших сервісів. У статті досліджено питання кібербезпеки трьох популярних сервісів відео-конференц-зв'язку, а саме: Microsoft Team, Zoom та Google Meet. Проаналізовано особливості роботи цих сервісів та найбільший акцент поставлено на стан забезпечення захисту інформації. З'ясовано, якими протоколами забезпечено передавання голосової та відеоінформації, як забезпечено захист від несанкціонованого доступу та особливості налаштування таких ресурсів. Здійснено порівняння розглянутих сервісів на основі критеріїв безпеки. Проаналізовано проблеми, які виникали під час використання сервісів відеозв'язку. Зрозуміло, що немає ідеального інструменту відеоконференцій - остаточний вибір завжди залежить від потреб користувача. У результаті дослідження виявлено, що більш безпечним є використання сервісів Google Meet та Microsoft Teams. Наведено рекомендації, які допоможуть захистити онлайн-зустрічі на основі кращих практик. Варто зазначити, що дотримання правил онлайн-гігієни для відеоконференцій дасть змогу ефективно та безпечно працювати навіть у найскладніші періоди.

Ключові слова: віртуальний простір; сервіс відеозв'язку; кібербезпека

ВСТУП

Спалах коронавірусної хвороби (COVID-19) спричинив ізоляцію людей від родини, друзів та ділових партнерів. Ця ситуація сприяла різкому збільшенню рівня використання відеоконференцій для різних цілей у бізнесі, навчанні та особистому житті людини. Пандемія змушує більшість із нас працювати і навчатися вдома, а також відвідувати віртуальні сімейні та соціальні заходи. Як результат, освітяни та споживачі звертаються до більш масштабних, більш надійних рішень для відеоконференцій

корпоративного рівня. В час пандемії сервіси, які дають можливість проводити відео-зустрічі, забезпечують злагоджений процес роботи команд, персоналу різноманітних фірм, а також викладачів та учнів. Висока різноманітність таких програм є причиною конкуренції, постійного вдосконалення та боротьби за безпечний зв'язок. Як і будь-яка інформаційна система, система відеозв'язку може опинитися під загрозою: витік інформації під час переговорів, хакерські атаки, вандалізм чи під'єднання користувача, з неадекватною поведінкою, з метою дестабілізації наради або ж випадкові дії користувачів чи адміністраторів.

Відеоконференції допомагають добитися максимальної присутності всіх учасників, не відриваючи їх від робочих місць, або ж продовжувати робочий процес дотримуючись норм ізоляції. Такі платформи вже давно стали рішеннями, які демонструють фінансові та адміністративні переваги, особливо для великих, розділених на філіали фірм. Можливість, не покидаючи домівки, злагоджено працювати над командними проектами чи завданнями, збільшує продуктивність, ефективність, економить час, також зростає конкурентоспроможність, яка приводить до результативності та прибутку.

Постановка проблеми.

В час пандемії сервіси, які дають можливість проводити відео-зустрічі, забезпечують злагоджений процес роботи команд, персоналу різноманітних фірм, а також викладачів та учнів. Висока різноманітність таких програм є причиною конкуренції, постійного вдосконалення та боротьби за безпечний зв'язок. Як і будь-яка інформаційна система, система відеозв'язку може опинитися під загрозою: витік інформації під час переговорів, хакерські атаки, вандалізм чи під'єднання користувача, з неадекватною поведінкою, з метою дестабілізації наради або ж випадкові дії користувачів чи адміністраторів. Так, наприклад, у квітні 2020 року на YouTube і Vimeo [1] з'явилися у відкритому доступі записи особистих відеодзвінків користувачів Zoom, у числі шкільні уроки, психотерапевтичні сеанси і консультації лікарів, а також корпоративні наради. З огляду на вище написане перед нами постало питання дослідити стан кібербезпеки сучасних ресурсів, які масово використовуються у теперішній час.

Аналіз останніх досліджень і публікацій. З моменту переходу у дистанційну роботу питання вибору безпечного сервісу відеозв'язку цікавило багатьох. Аналізуючи матеріали закордонних інтернет видань «Digital Information World» [2], «Business Insider» [3], Journal of Accountancy [4] та вітчизняних «Techno (IT-індустрія)) [5] та «Українська правда» [6] питання сервісів відеозв'язку є доволі актуальним, оскільки, у цей час люди масово використовують є доволі актуальним питанням. Проте зазвичай у матеріалах описується базові характеристики сервісів, так як, кількість користувачів у нараді,

Метою статті є аналіз рівня кібербезпеки популярних ресурсів відеозв'язку, що дає змогу зрозуміти, який є найбільш безпечний.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У статті ми розглянули 3 популярніші сервіси для відеоконференцій на 2021 рік, такі як: Microsoft Teams, Zoom та Google Meet.

Проблеми безпеки для будь-якої конференц-платформи є реальними. Навіть у 2020 році такі компанії, як Google Nest та Zoom, все ще роблять хакерам відносно легкий доступ до своїх потокових відеофільмів. Відеоконференції та відеопристрої IoT є важливими цілями, і, поєднуючи незахищені мережі та додаткові методи безпеки для

відеоконференцій, можливе відкриття особи та її особистих даних чи бізнесу перед зловмисниками.

Аналіз Microsoft Teams

Microsoft Teams – платформа для співпраці за допомогою відеоконференцій, дзвінків та переписок, яку станом на січень 2021 року вже використовували 75 мільйонів щоденних активних користувачів для ведення бізнесу, навчання та особистого користування [7-9]. Розроблена компанією Microsoft платформа була покликана, щоб замінити Skype for Business, конкуруючи на той час з програмою Slack, яка невпинно втрачає своїх користувачів.

Зручність Microsoft Teams полягає у вбудованій в платформу функції та можливості Office 365, так як: Word, Excel, Powerpoint, SharePoint, OneNote, команди можуть колективно створювати документи, редагувати та коригувати свої проекти чи презентації, спільно працювати в інших додатках. За потреби можна створити особистий чат, а також здійснювати дзвінки окремо тому чи іншому члену команди.

Засоби контролю конфіденційності та безпеки для відеоконференцій у Teams [8-10]:

- *Варіанти зустрічей:* за допомогою варіантів зустрічей користувач може вирішити, хто з-за меж організації може безпосередньо приєднуватися до планових зустрічей, а хто повинен чекати у вестибюлі;
- *Ролі на засіданні:* організатор наради може визначити ролі на засіданні команд, які визначають «ведучих» та «учасників», а також контролювати, яким учасникам наради дозволено представляти вміст на засіданні;
- *Згода учасників на запис:* записи зустрічей супроводжуються повідомленням учасникам про те, що запис відбувається;
- *Багатофакторна автентифікація:* вимагає від користувачів додаткових форм перевірки, щоб підтвердити свою особу, допомагаючи захистити свої акаунти від атак, які використовують переваги слабких або викрадених паролів;
- *Умовний доступ:* дає змогу встановлювати політики доступу на основі ризику на основі контексту користувача, стану пристрою, розташування тощо;
- *Microsoft Endpoint Manager*: дає можливість користувачу керувати пристроями та програмами та застосовувати умовний доступ на будь-якому пристрої;
- *Безпечний гостьовий доступ:* забезпечує можливість користувачам співпрацювати з особами, які не належать до їх організації, одночасно контролюючи їхній доступ до даних організації;
- *Зовнішній доступ:* забезпечує автентичне з'єднання з іншою організацією, що забезпечує співпрацю між організаціями;
- *Розширений захист від загроз:* допомагає захистити користувачів від шкідливого програмного забезпечення, прихованого у файлах, включаючи файли, що зберігаються в OneDrive або SharePoint;
- *Cloud App Security:* надає інструменти для виявлення та зменшення підозрілої або шкідливої діяльності, включаючи масштабне видалення команд або додавання неавторизованих користувачів;
- *Захист від несанкціонованого доступу:* щоб забезпечити відсутність прямого чи необмеженого доступу до даних.

ISSN 2663 - 4023

Шифрування в MS Teams

Особливе місце займає шифрування даних у MS Teams. З'ясовано, що для шифрування миттєвих повідомлень використовується TLS (Transport Layer Security, захист на транспортному рівні) та MTLS (Manual TLS, взаємна автентифікація) [8-10].

TLS – криптографічний протокол, який заснований на протоколі SSL (Secure Sockets Layer), надає можливості безпечної передачі даних в інтернеті для навігації, отримання пошти, спілкування, обміну файлами, тощо. Використовує асиметричне шифрування і сертифікати X.509. Весь трафік вимагає MTLS, незалежно від того, обмежений трафік внутрішньою мережею чи перетинає периметр внутрішньої мережі. TLS і MTLS допомагають запобігти перехоплення повідомлень та атаки типу "man-in-the-middle".

Медіа-трафік шифрується за допомогою безпечного RTP/SRTP (Secure Real-time Transport Protocol), протокол передачі даних в реальному часі визначає профіль RTP (транспортний протокол реального часу) і призначений для шифрування, встановлення автентичності повідомлення, цілісності, захисту від заміни даних RTP в unicast і multicast передачах медіа і додатках. Цей протокол забезпечує конфіденційність, автентифікацію та захист від повторних атак для трафіку RTP.

Таблиця 1

Узагальнення протоколів, які використовуються Teams

Тип трафіку	Захищений протокол
Сервер	MTLS
Клієнт-сервер (наприклад, обмін миттєвими повідомленнями та присутність)	TLS
Медіапотоки (аудіо- та відеозв'язок, мультимедіа)	TLS
Обмін аудіо та відео медіа	SRTP / TLS
Сповіщення	TLS

Аналіз Zoom

Zoom – це сервіс для проведення відеоконференцій та онлайн-зустрічей. Zoom допомагає компаніям та організаціям об’єднувати свої команди, щоб зробити більше. Проста в користуванні хмарна платформа для відео та голосового зв'язку, обміну різноманітним вмістом працює практично на будь-якій платформі. Організувати зустріч може будь-який користувач, який має обліковий запис.

Аналіз особливостей функціонування, засобів контролю конфіденційності та безпеки для відеоконференцій у Zoom [11-12]:

- *Зали очікування.* адміністратор зустрічі може примусово включити зал очікування на рівнях облікового запису, групи або користувача;
- *Паролі*. Паролі можна задати на рівні окремих конференцій або ж на рівні користувача, групи або облікового запису для всіх конференцій та вебінарів;
- *Вхід по домену.* Приєднатися до онлайн зустрічі можуть лише авторизовані користувачі;
- *Налаштування безпеки на панелі інструментів*. Ця функція дає змогу отримати швидкий доступ до важливих функцій безпеки у конференції;
- *Блокування конференції.* Якщо організатор блокує вже розпочату конференцію Zoom, до неї не зможуть приєднуватися інші учасники;

- *Вимкнути звук учасників.* Організатор може вимкнути звук для всіх або окремих учасників. Організатор може блокувати небажаний, відволікаючий або неналежний шум від інших учасників;
- *Вимкнути приватний чат.* Zoom дає можливість використовувати загальнодоступний чат в конференції, або ж учасники можуть надсилати один одному приватні повідомлення;
- *Заборона на перейменування ідентифікаторів.* Організатор може заборонити учасникам змінювати свої екранні імена.

Шифрування в Zoom

Zoom пропонує багатофункціональний пакет клієнтського програмного забезпечення для комп'ютерів Mac і пристроїв з операційними системами Windows, iOS, Android і Linux, який використовує широкий перелік технологій шифрування для забезпечення конфіденційності та безпеки користувачів. Всі дані клієнтів, що передаються з клієнтського застосування в хмару Zoom, шифруються при передачі за допомогою одного з наступних методів.

TLS 1.2 – при створенні з'єднань між клієнтом Zoom і хмарою Zoom кращим способом зв'язку є протокол HTTPS. Ці сполуки використовують шифрування TLS 1.2 і сертифікати PKI, видані довіреним комерційним центром сертифікації. Деякі з поширених сценаріїв використання - вхід в клієнтську програму, планування конференції, спілкування в чаті, участь в опитуваннях, надання загального доступу до файлів і організація сеансів питань і відповідей в конференції. TLS 1.2 також виступає в якості резервного протоколу для інших комунікаційних потоків, наприклад, для передачі вмісту конференцій в реальному времені [11-13].

AES – у таких сценаріях використання, як передача вмісту конференції в реальному часі (відеоданих, голосових даних і матеріалів для спільного використання), де здійснюється передача даних по протоколу передачі дейтаграм UDP, використовується шифрування AES-256 в режимі ECB для захисту цих стислих потоків даних. Крім того, після шифрування відеоданих, голосових даних і матеріалів для спільного використання за стандартом AES вони залишаються зашифрованими при проходженні через сервери конференції Zoom до тих пір, поки не досягнуть іншого клієнта Zoom або коннектора Zoom, що здійснює трансляцію даних в інший протокол SRTP [9].

Окрім шифрування TLS, веб-сайт компанії Zoom в певних сценаріях може використовувати додаткове шифрування. Наприклад, клієнтські дані, до складу яких входять записи в хмарі, історія чатів і метадані конференцій, шифруються при зберіганні за стандартом AES-256 GCM з використанням хмарної системи управління ключами шифрування (KMS).

При підключенні користувача до конференції за допомогою веб-клієнта Zoom, що використовує веб-збірку, платформа Zoom буде відправляти і отримувати вміст конференції в реальному часі (відео, голосові дані і матеріали для спільного використання) по протоколу передачі дейтаграм UDP безпосередньо з сервера конференції, що використовує шифрування за стандартом AES-256 ECB [11-13].

Проблеми, що виникали з використанням

Попри зручність у користуванні Zoom, було виявлено проблеми безпеки протягом останнього часу, зокрема, відповідно до даних дослідження The Intercept [14], сервіс не здійснює наскрізне шифрування відео та аудіоконференцій, попри те, що в Zoom довгий час стверджували протилежне. Zoom заявляли, що всі відео дзвінки захищені шифруванням, проте в дійсності все не так красиво: сервіс дійсно використовує шифрування, але сеансовий ключ клієнтська програма запитує у одного з серверів

«системи управління ключами», що входять до складу хмарної інфраструктури Zoom. Ці сервери генерують ключ шифрування і видають його абонентам, які підключаються до конференції - один ключ для всіх учасників конференції. Передача ключа від сервера до клієнта відбувається через протокол TLS, який також використовується для https.

Частина серверів системи управління ключами розташована в Китаї, причому вони використовуються для видачі ключів, навіть коли всі учасники конференції знаходяться в інших країнах. Виникають справедливі побоювання, що уряд КНР може перехопити зашифрований трафік, а потім розшифрувати його за допомогою ключів, отриманих від провайдерів в добровільно-примусовому порядку.

Проблеми з шифруванням також пов'язана з його практичною реалізацією: хоча в документації вказано, що використовуються 256-бітові ключі AES, їх фактична довжина становить лише 128 біт; алгоритм AES працює в режимі ECB, при використанні якого результат шифрування частково зберігає структуру вихідних даних.

Також було встановлено, що додаток містить декілька вразливостей безпеки, які компанія швидко виправила та випустила оновлення. Зокрема, у версії додатка для Windows була уразливість введення маршруту UNC, яка могла призвести до витоків облікових даних користувачів і навіть до виконання довільних команд на їх пристроях.

Компанії також довелося відмовитися від функції «відстеження відвідувачів», яка давала можливість власнику конференції перевірити, чи дійсно учасники уважно дивились трансляцію, коли він використовував режим обміну екраном.

Аналіз Google Meet

Google Meet, також відомий як Google Hangouts Meet, створений для того, щоб дати можливість десяткам людей приєднуватися до однієї і тієї ж віртуальної зустрічі та розмовляти або обмінюватися відео між собою з будь-якого місця з доступом до Інтернету.

Організатор Google Meet може ділитися тим, що є на їх екрані, з усіма під час дзвінка, і будь-який учасник може у будь-який час вимкнути власну аудіо та / або відеопотоку, беручи участь, як завгодно [15].

Засоби контролю конфіденційності та безпеки для відеоконференцій у GMeet [16]:

- всі комунікації між клієнтом і хмарними серверами шифруються, сервіс підтримує стандарти безпеки IETF для Datagram Transport Layer Security і Secure Real-time Transport Protocol;
- реалізований ряд обмежень для зовнішніх учасників, що підключаються до конференції через код зустрічі;
- вхід користувачів в конференцію повинен бути схвалений адміністратором, а саме підключення стає доступним лише за 15 хвилин до початку наради;
- управління користувальницької інформацією реалізовано в рамках стандартної політики конфіденційності для продуктів Google і допускає видалення інформації як з сервера, так і з клієнтського пристрою.
- суттєвий недолік: не підтримує наскрізне шифрування даних, що залишає зловмисникам можливість перехоплення інформації.
- ускладнює атаку методом перебору (brute force) ідентифікаторів нарад (це коли зловмисна особа намагається вгадати ідентифікатор наради та зробити несанкціоновану спробу приєднатися до неї), використовуючи коди довжиною 10 символів із набором 25 символів;
- лише творці зустрічей та власники календарів можуть ігнорувати або видаляти інших учасників, схвалювати запити на приєднання від зовнішніх учасників.

Безпечне розгортання та контроль доступу для адміністраторів та кінцевих користувачів

Щоб обмежити можливості для атаки та усунути необхідність випускати часті виправлення безпеки, Google Meet працює повністю у вашому браузері . Це означає, що компанія не вимагає встановлення будь-яких плагінів чи програмного забезпечення, якщо користувач використовує Chrome, Firefox, Safari або Microsoft Edge. На мобільних пристроях рекомендується встановити додаток Google Meet.

Компанія підтримує кілька варіантів двоетапної перевірки для безпечних та зручних облікових записів. Сюди входять апаратні та телефонні ключі безпеки та запит Google. Крім того, користувачі Google Meet можуть зареєструвати свій обліковий запис у Програмі розширеного захисту, яка забезпечує найсильніший захист від фішингу та викрадення облікового запису та спеціально розроблена для облікових записів з найвищим ризиком.

Порівняння сервісів відеозв'язку

Розглянемо порівняльну таблицю (табл. 2) сформовану на основі ключових критеріїв безпеки, а саме - шифрування, МФА, кімната очікування, функції контролю даними, управління відеоконференціями, а також кількість вразливостей.

Таблиця 2

Порівняння розглянутих сервісів на основі критеріїв безпеки

	MS Teams	**Zoom**	**GMeet**
Шифрування даних	+	+	+
Двохфакторна автентифікація	+	-	+
Наявність кімнати очікування	+	+	+
Функція управління персональними даними	+	+	+
Кількість вразливостей за Mitre	1	14	0

Як видно з табл. 2 найбільш платформа Zoom з точки зору кібербезпеки є менш безпечною, оскільки уже виявлено 14 вразливостей, відсутня двохфакторна автентифікація та шифрування. А GMeet та MS Teams є більш безпечними. Наведемо деякі правила, які допоможуть захистити онлайн-зустрічі:

- використовувати останню версію ПО;
- завантажувати установники програм тільки з офіційних ресурсів;
- не публікувати ID зустрічей в інтернеті;
- захистити облікові записи за допомогою двофакторної автентифікації;
- надавати можливість підключення до зустрічей лише авторизованим користувачам;
- закрити можливість нових підключень після початку заходу;
- включити для організатора можливість блокувати або видаляти учасників зустрічі;
- використовувати сучасні антивірусні рішення, що забезпечують комплексний захист від нових і відомих загроз.

Дотримання правил онлайн-гігієни для відеоконференцій [17] дасть змогу ефективно та безпечно працювати навіть у найскладніші періоди.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті здійсненого дослідження сервісів відеозв'язку Zoom, MS Teems, Google Meet. Як з'ясувалось, кожен з розглянутих об'єктів має переваги та недоліки. Після порівняння забезпечення безпеки та конфіденційності, виявлено, що більш безпечними є Google Meet та MS Teams.

Базові вимоги до сервісів для організації відеоконференцзв'язку – якість, надійність і безпеку. І якщо перші дві вимоги в основному можна порівняти у всіх великих гравців, то ситуація з безпекою значно відрізняється. Тому подальшим напрямом дослідження є розробка нових методів захисту сервісів відеозв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Thousands of Zoom video calls left exposed on open Web. https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web
2 Zoom vs. Google Meet vs. Microsoft Teams: New data reveals the World`s most popular video calling platform. https://www.digitalinformationworld.com/2021/04/top-video-call-platform-by-market-share.html
3 Christian de Looper, Ben Blanchet, Steven Cohen. Google Meet vs. Zoom: Here's how the popular video conferencing tools stack up. https://www.businessinsider.com/google-meet-vs-zoom
4 Byron Patrick. Zoom vs. Teams vs. Google Meet: Which is right for you? https://www.journalofaccountancy.com/issues/2021/feb/compare-zoom-teams-google-meet.html
5 Zoom проти Skype - який сервіс для відеоконференцій краще. https://techno.nv.ua/ukr/it-industry/zoom-abo-skype-yakiy-servis-krashche-porivnyannya-plyusi-i-minusi-50094378.html
6 Найкращий сервіс для віддаленої освіти. https://life.pravda.com.ua/columns/2020/05/12/240947/
7 Тихолаз Д. Аналіз захищеності сервісів відеозв'язку / Д. Тихолаз, І. Бумба, М. Шабатура // Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів 27 листопада 2020 року, Львів, ЛДУ БЖД, 2020, С. 48-507.
8 Bradley S. (2019). Security and compliance considerations for Microsoft Teams. https://www.csoonline.com/article/3436940/security-and-compliance-considerations-for-microsoft-teams.html
9 Say M. (2020) NCSC produces security guidance for video conferencing. https://www.ukauthority.com/articles/ncsc-produces-security-guidance-for-video-conferencing/
10 Безпека MS Teams. https://www.csoonline.com/article/3436940/security-and-compliance-considerations-for-microsoft-teams.html
11 Безпека та приватність. Офіційний сайт Zoom. https://zoom.us/privacy-and-security
12 Безпека Zoom.https://www.itgovernance.co.uk/blog/is-zoom-safe-to-use
13 Lee M, Grauer Y. (2020). Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing. https://theintercept.com/2020/03/31/zoom-meeting-encryption/
14 Zoom. https://theintercept.com/2020/03/31/zoom-meeting-encryption/
15 Відеоконференції в Google Meet. https://workspace.google.com/products/meet/
16 Захист та приватність Google Meet. Офіційний сайт Google. https://support.google.com/a/answer/7582940?hl=en
17 Bitterli J. (2020). How Secure Is Video Conferencing? https://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-secure-is-video-conferencing/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Mariia M. Shabatura
PhD, Associate Professor, Associate Professor of Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0003-0814-1855
mariia.m.mandrona@lpnu.ua

Dmytrii O. Tykholaz
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0003-1014-5601
dtykholaz@email.com

Irina Y. Bumba
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID 0000-0002-1983-7260
bumba.iryna.2002@gmail.com

INVESTIGATION CYBER SECURITY STATE OF VIDEO COMMUNICATION SERVICES

Abstract. Online meeting services are great resources that are now saving the world during a pandemic. This is a key component that helps many businesses continue operating, universities, colleges and schools continue teaching, even family and friends can stay in touch during isolation. Video conferencing is a telecommunication technology of interaction for three or more remote users, in which between them it is possible to exchange audio and video information in real time, taking into account the transfer of control data. To date, there are many such resources, but the question arises "who to trust", because in the news there is often information about data breaches due to the vulnerability of certain services. The article examines the issues of cybersecurity of three popular video conferencing services, such as: Microsoft Team, Zoom and Google Meet. The peculiarities of the work of these services are analyzed and the greatest emphasis is placed on the state of information security. It is found out what protocols ensure the transmission of voice and video information, how protection against unauthorized access is provided and the peculiarities of setting up such resources. The considered services are compared on the basis of security criteria. Analyzed issues that occurred while using video services. It is clear that there is no perfect video conferencing tool - the final choice always depends on the needs of the user. The study found that it is safer to use Google Meet and Microsoft Teams. Here are tips to help protect online meetings based on best practices. It is worth noting to follow the rules of online hygiene for video conferencing, that will allow you to work efficiently and safely even in the most difficult periods.

Keywords: virtual space; video communication services; cybersecurity

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Thousands of Zoom video calls left exposed on open Web. https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web
2 Zoom vs. Google Meet vs. Microsoft Teams: New data reveals the World`s most popular video calling platform. https://www.digitalinformationworld.com/2021/04/top-video-call-platform-by-market-share.html
3 *Christian de Looper, Ben Blanchet, Steven Cohen.* Google Meet vs. Zoom: Here's how the popular video conferencing tools stack up. https://www.businessinsider.com/google-meet-vs-zoom
4 *Byron Patrick.* Zoom vs. Teams vs. Google Meet: Which is right for you? https://www.journalofaccountancy.com/issues/2021/feb/compare-zoom-teams-google-meet.html

5 Zoom proty Skype - yakyi servis dlia videokonferentsii krashche.https://techno.nv.ua/ukr/it-industry/zoom-abo-skype-yakiy-servis-krashche-porivnyannya-plyusi-i-minusi-50094378.html
6 Naikrashchyi servis dlia viddalenoi osvity. https://life.pravda.com.ua/columns/2020/05/12/240947/
7 *Tykholaz D., Bumba I., Shabatura M.* Analiz zakhyshchenosti servisiv videozviazku // *Informatsiina bezpeka ta informatsiini tekhnolohii: zbirnyk tez dopovidei IV Vseukrainskoi naukovo-praktychnoi konferentsii molodykh uchenykh, studentiv i kursantiv* 27.11.2020, Lviv, LDU BZhD, 2020, S. 48-507.
8 Bradley S. (2019). Security and compliance considerations for Microsoft Teams. https://www.csoonline.com/article/3436940/security-and-compliance-considerations-for-microsoft-teams.html
9 *Say M.* (2020) NCSC produces security guidance for video conferencing. https://www.ukauthority.com/articles/ncsc-produces-security-guidance-for-video-conferencing/
10 MS Teams Security. https://www.csoonline.com/article/3436940/security-and-compliance-considerations-for-microsoft-teams.html
11 Security & Privacy. Official site. https://blog.zoom.us/category/company-news/security-privacy/?_ga=2.152568762.288035773.1632402284-1556754990.1631992352
12 Zoom Security.https://www.itgovernance.co.uk/blog/is-zoom-safe-to-use
13 *Lee M, Grauer Y.* (2020). Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing. https://theintercept.com/2020/03/31/zoom-meeting-encryption/
14 Zoom. https://theintercept.com/2020/03/31/zoom-meeting-encryption/
15 Google Meet Video conferencing. https://workspace.google.com/products/meet/
16 Google Meet protection and privacy. Official site. https://support.google.com/a/answer/7582940?hl=en
17 *Bitterli J.* (2020). How Secure Is Video Conferencing? https://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-secure-is-video-conferencing/