Ганна Скрипка
кандидатка педагогічних наук, завідувачка кафедри інформаційно-комунікаційних технологій та безпечного освітнього середовища комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського», м. Кропивницький, Україна

Олександр Скрипка
викладач кафедри тактико-спеціальної підготовки факультету №2 Донецького державного університету внутрішніх справ, м. Кропивницький, Україна

АНАЛІЗ ІНСТРУМЕНТІВ ВІДЕОЗВ'ЯЗКУ ДЛЯ ОРГАНІЗАЦІЇ СИНХРОННОГО ОНЛАЙН НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ СИСТЕМИ МВС

Нові виклики, що пов'язані з упровадженням воєнного стану на території України, змушують заклади освіти адаптовуватися під них та шукати ефективні шляхи навчання, поєднуючи очне навчання з дистанційним. Дистанційне навчання для окремих категорій здобувачів закладів вищої освіти системи МВС організовується шляхом поєднання синхронної та асинхронної взаємодії й особливо актуальним є питання безпеки всіх учасників освітнього процесу в умовах війни.

Синхронне навчання на відстані забезпечується з допомогою засобів відеозв'язку й тому **метою** нашого **дослідження** є виокремлення таких інструментів, які забезпечать безпечну роботу здобувачів освіти системи МВС в умовах воєнного стану.

Згідно з Положенням про організацію дистанційного навчання, під **дистанційним навчанням** розуміється індивідуалізований процес набуття знань, умінь, навичок і способів пізнавальної діяльності людини, який відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників навчального процесу у спеціалізованому середовищі, яке функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій [1]. **Змішане навчання** – це навчання, за якого частина навчальної діяльності здобувачів освіти відбувається на занятті під безпосереднім керівництвом викладача, а інша – у самостійній роботі з електронними ресурсами [2].

Найоптимальнішим інструментом, який дозволяє організувати навчання на відстані та який і є тим спеціалізованим середовищем, є **платформа дистанційного навчання** (наприклад, Moodle, яку успішно використовує Донецький державний університет внутрішніх справ – https://osvita.dduvs.in.ua/), проте для підвищення якості викладання доречно використовувати засоби відеозв'язку, які здатні доповнити можливості платформи дистанційного навчання та вивести викладання на якісно новий рівень.

В умовах війни розголошення будь-якої конфіденційної інформації щодо громадян, військовослужбовців, поліцейських та інших груп населення, може

призвести до обізнаності противника, негативно вплинути на хід виконання завдань за призначенням.

Забезпечення безпеки здобувачів освіти під час онлайнових занять з використанням відеозв'язку для у закладах освіти системи МВС є критично важливим з ряду причин:

конфіденційність інформації (можливе обговорення особистих та конфіденційних даних під час відеозв'язку – адреси проживання, інформації про службу в армії чи органах МВС рідних, знайомих, друзів);

несанкціонований доступ (ризик несанкціонованого доступу осіб, які не є учасниками занять, що може призвести до порушень приватності та недозволених втручань у навчальний процес);

захист від кіберзагроз (ймовірність хакерських атак, вірусів та інших шкідливих програм).

Таким чином, закладами освіти системи МВС має бути забезпечено безпечне та надійне середовище для відеозв'язку, яке дозволить ефективно взаємодіяти та обмінюватися інформацією в межах освітнього процесу, забезпечуючи конфіденційність та безпеку всім учасникам.

Розглянемо найбільш популярні платформи відеозв'язку.

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 [3].

Засоби контролю конфіденційності та безпеки для відеоконференцій у Teams забезпечуються шляхом вибору варіанту зустрічей, визначення ролей на засіданні («ведучі» та «учасники», а також учасники, яким дозволено представляти вміст на засіданні), згоди учасників на запис, багатофакторної автентифікації, умовного доступу (встановлювлення політики доступу на основі контексту користувача, стану пристрою, розташування тощо), Microsoft Endpoint Manager (керування пристроями та програмами та застосовування умовного доступу на будь-якому пристрої), безпечного гостьового доступу, зовнішнього доступу (автентичне з'єднання з іншою організацією, що забезпечує співпрацю між організаціями), розширеного захисту від загроз (захист користувачів від шкідливого програмного забезпечення, прихованого у файлах, включаючи файли, що зберігаються в OneDrive або SharePoint), Cloud App Security (інструменти для виявлення та зменшення підозрілої або шкідливої діяльності, включаючи масштабне видалення команд або додавання неавторизованих користувачів), захисту від несанкціонованого доступу.

У MS Teams для шифрування миттєвих повідомлень використовується TLS (Transport Layer Security, захист на транспортному рівні) та MTLS (Manual TLS, взаємна автентифікація) [3].

Не менш популярним серед користувачів є інструмент **Zoom** – сервіс для проведення відеоконференцій та онлайн-зустрічей. У відеоконференціях Zoom використовуються такі засоби контролю конфіденційності та безпеки [5]: зали очікування (примусове включення залу очікування на рівнях облікового запису, групи або користувача), паролі, вхід по домену (приєднання до онлайн зустрічі

виключно авторизованих користувачів), налаштування безпеки на панелі інструментів, блокування конференції (неможливість приєднання інших учасників), вимкнення звуку учасників, вимкнення приватного чату, заборона на перейменування ідентифікаторів.

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) [3]. Проте, наскрізне шифрування Zoom meetings не працює на 100%, результатом чого стали непоодинокі випадки зумбомбінгу, які не припинилися навіть після доопрацювання наскрізного шифрування у 2022 році [7].

Google Meet – сервіс відеозв'язку, розроблений компанією Google, який є одним із найбільш популярних серед закладів освіти. Засоби контролю конфіденційності та безпеки для відеоконференцій у Google Meet представлені наступними функціями [6]: шифрування серверами всіх комунікацій між клієнтом і хмарними (підтримка стандартів безпеки IETF для Datagram Transport Layer Security і Secure Real-time Transport Protocol), обмеження для зовнішніх учасників, що підключаються до конференції через код зустрічі, схвалення адміністратором входу користувачів в конференцію, ускладнення атаки методом перебору (brute force) ідентифікаторів нарад, можливість творцями зустрічей ігнорувати або видаляти інших учасників, схвалювати запити на приєднання від зовнішніх учасників.

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 [3].

Таким чином, інструменти відеозв'язку, які використовують учасники освітнього процесу в системі освіти МВС, мають бути надійними та безпечними, аби забезпечувати конфіденційність працівників органів внутрішніх справ, що є особливо актуальним в умовах воєнного стану.

Аналіз найбільш популярних засобів відеозв'язку показує, що кожен з них має свої переваги та недоліки з точки зору безпеки учасників освітнього процесу, проте більш безпечними є Google Meet та MS Teams, оскільки в Zoom відсутня двохфакторна автентифікація, а також наявні інші вразливості.

Перспективами подальших досліджень є вивчення альтернативних інструментів відеозв'язку на предмет безпеки використання, які є оптимальними для використання в закладах освіти системи МВС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Наказ МОН України від 25.04.2013 № 466 "Про затвердження Положення про дистанційне навчання» URL:

https://zakon.rada.gov.ua/laws/show/z0703-13#Text (дата звернення: 01.10.2023).

2. Змішане навчання: як організувати якісний освітній процес в умовах війни URL: https://sqe.gov.ua/zmishane-navchannya-yak-organizuvati-yaki/ (дата звернення: 01.10.2023).

3. Шабатура, М., Тихолаз, Д. ., & Бумба, І. (2021). ДОСЛІДЖЕННЯ СТАНУ КІБЕРБЕЗПЕКИ СЕРВІСІВ ВІДЕОЗВ'ЯЗКУ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(13), 113–122. https://doi.org/10.28925/2663-4023.2021.13.113122.

4. MS Teams Security. URL: https://www.csoonline.com/article/3436940/security-and-compliance-considerations-for-microsoft-teams.html (дата звернення: 01.10.2023).

5. Безпека та приватність. Офіційний сайт Zoom. URL: https://zoom.us/privacy-and-security (дата звернення: 01.10.2023).

6. Відеоконференції в Google Meet. URL: https://workspace.google.com/products/meet/ (дата звернення: 01.10.2023).

7. Чому Zoom може втратити «зумерів». URL: https://laba.ua/blog/3871-swot-analiz-zoom (дата звернення: 01.10.2023).