СЕКЦІЯ 17

ІНФОРМАТИЗАЦІЯ СУСПІЛЬСТВА ТА ЗАХИСТ ІНФОРМАЦІЇ

Керівник секції: *в. о. завідувача кафедри інформаційних технологій, к. пед. н., доцент Н.І. Логінова*

Секретар секції: *лаборант кафедри інформаційних технологій Р.С. Сікальська*

ЛОГІНОВА НАТАЛІЯ ІВАНІВНА

Національний університет «Одеська юридична академія», в.о. завідувача кафедри інформаційних технологій, кандидат педагогічних наук, доцент

ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОГРАМІ ZOOM

Технології дистанційного навчання вже досить давно поєднуються з традиційними формами аудиторного навчання, організовуючи змішане навчання. При такому навчанні використовуються елементи комп'ютерної графіки, подача навчальних матеріалів за допомогою текстових, аудіо- та відео- контентів, інтерактивні елементи та ін.

В умовах пандемії коронавірусу навчальні заклади змушені були перейти на дистанційне навчання. В ситуації, що склалася, викладачам довелося в короткі терміни освоювати сучасні інформаційні технології для активізації навчального процесу. Гостро постала проблема організації зворотного зв'язку між тими, хто навчається і викладачами. Багато освітніх установ вирішили проводити заняття онлайн за допомогою різних програм, призначених для відеоконференцій. Благо безкоштовних систем і онлайн сервісів відеоконференцій в мережі інтернет пропонується велика кількість. Єдиний недолік таких програм, з точки зору користувача – це обмеження за часом і кількістю учасників, но для проведення дистанційних занять таки сервіси повністю задовольняють. Однак, в даної ситуації користувачі не звернули увагу на питання інформаційної безпеки та захисту конференційної інформації.

Як показує аналіз програм, які використовуються в навчальному процесі для відеоконференцій, найбільш поширеною є програма Zoom. Даний сервіс був розроблений в 2011 році компанією Zoom

Video Communications для проведення хмарних відеоконференцій, веб зустрічей, чатів і спільної мобільної роботи користувачів.

В основі своєї роботи додаток використовує стандарт шифрування TLS (Transport Layer Security – протокол захисту транспортного рівня), який застосовується веб-браузерами для захисту з'єднання з сайтами через протокол HTTPS. Цей стандарт реалізує властивості інформації, що визначають стан її безпеки:

– шифрування – приховування інформації, що передається, за допомогою кодування;
– аутентифікацію – перевірка авторства переданої інформації;
– цілісність – визначає існування інформації в незмінному стані в певний проміжок часу.

Протокол TLS використовує асиметричне шифрування для аутентифікації, симетричне шифрування для забезпечення конфіденційності та коди автентичності повідомлень для збереження цілісності повідомлень. Його недоліком, в першу чергу є те, що для транспортування повідомлень використовується тільки один протокол мережевого рівня IP. Відповідно, захисні властивості даного протоколу не в повній мірі прозоро для прикладних протоколів. Також при використанні протоколу TLS, можливе відновлення сесій. Тобто, при розриві з'єднань клієнт і сервер можуть відновити його, провівши мінімальний обмін даними, і використовувати старий параметр сесії. Це дозволяє зловмисникові, який спровокував розрив з'єднання, провести процедуру відновлення та перехоплювати дані, передані в процесі використання програми. Крім того, для аутентифікації та шифрування в протоколі використовуються однакові ключі, що за певних умов може призвести до уразливості інформації. Протокол TLS схильний до кібератак, пов'язаним з недостовірним програмним середовищем, впровадженням програм-закладок та ін. [1].

Для того, щоб забезпечити захист передачі інформації в програмі Zoom необхідно використовувати захист наскрізного шифрування E2E (End-to-end), яке полягає в тому, що кінцевими пунктами передачі є безпосередньо пристрою відправника і одержувача. Повідомлення шифрується на пристрої відправника і може бути розшифровано тільки на пристрої одержувача. Таким чином, шифрування відбувається на пристроях кінцевих користувачів, а не на хмарних серверах, що запобігає потенційному читанню призначених для користувача даних серверами. При реалізації шифрування E2E використовуються симетричний і асиметричний криптографічні алгоритми, що й забезпечує максимальний рівень захисту інформації користувачів.

На офіційному сайті програми Zoom зазначено про використання такого виду шифрування, але сам представник платформи спростовує цю інформацію вказуючи, що в даний час неможливо включити шифрування E2E для відеоконференцій. Для збільшення масштабу відео зустрічей використовується комбінація TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). TCP-з'єднання виконуються з використанням TLS, а UDP-з'єднання шифруються за

допомогою AES з використанням ключа, узгодженого через TLS-з'єднання.

Небезпека витоку інформації користувачів полягає в самому способі підключення до конференцій. Шляхи до файлів в чатах Zoom перетворюються на гіперпосилання. При натисканні на сформований URL клієнт автоматично відправляє логін і хеш-пароль NTLM, до яких можуть отримати доступ злочинці. Також в програмі можна технічно отримати доступ до приватних відеоконференцій, і компанія-розробник може передавати ці записи стороннім особам [2].

Для доступу до відеоконференції програма випадково генерує ідентифікатори довжиною від 9 до 11 цифр, який використовується учасниками. Дослідження фахівців показало, що ці ідентифікатори легко вгадати шляхом простого перебору, дозволяючи будь-якому підключатися в конференції.

Все це й стало причиною скандалу в квітні 2020 року, коли кіберзлочинці змогли прослуховувати відеоконференції, отримали доступ до всіх аудіо та відеофайлів, а також документів, якими обмінювалися користувачі. Персональні дані користувачів, а це – електронні адреси, паролі, адреси приватних чатів та ін., передавалися стороннім компаніям, зокрема, Facebook та YouTube. Також уразливість дозволила зловмисникам отримувати доступ до управління комп'ютерами та гаджетами, а також особистих файлів користувачів програми.

У компанії визнали провину і спробували змінити систему безпеки в групових дзвінках: зокрема, став обов'язковим введення пароля, а також з'явилися «кімнати очікування», за допомогою яких учасники конференції зможуть заборонити доступ до чату небажаним особам [3].

Отже, використовуючи в навчальному процесі платформу відеоконференцій Zoom користувачі можуть зіткнутися з витоком конфіденційної інформації. Тому користувачі програми повинні контролювати питання безпеки – використовувати програми-брандмауери, міжмережеві екрани, антивірусне програмне забезпечення. В самої програми необхідно використовувати паролі для відеоконференцій, застосовувати обмеження доступу до екрану, постійно стежити за оновленнями програми, так як розробник постійно вдосконалює систему захисту.

Список використаної літератури:

1. Венедюх А. Ключи, шифры, сообщения: как работает TLS [Електронний ресурс] – Режим доступу до ресурсу: https://tls.dxdt.ru/tls.html. – Назва з екрана. – Дата перегляду: 10.04.2020.
2. Micah Lee, Yael Grauer. Zoom meetings aren't end-to-end encrypted, despite misleading marketing [Електронний ресурс] – Режим доступу до ресурсу: https://theintercept.com/2020/03/31/zoom-meeting-encryption/?fbclid=IwAR3n2tacvOVnIOJcIxVJRNflNINB1VCtWGImXorlSPe7ZIBc248Z9e9cH0g. – Назва з екрана. – Дата перегляду: 10.04.2020.

3. Опанасенко Е. Конференции в Zoom оказались под угрозой: хакеры воруют пароли [Електронний ресурс] – Режим доступу до ресурсу: https://www.segodnya.ua/lifestyle/science/konferencii-v-zoom-okazalis-pod-ugrozoy-hakery-voruyut-paroli-1425732.html. – Назва з екрана. – Дата перегляду: 10.04.2020.

Ключові слова: конфіденційна інформація, відеоконференція, інформаційна безпека, шифрування.
Ключевые слова: конфиденциальная информация, видеоконференция, информационная безопасность, шифрование.
Key words: confidential information, video conferencing, information security, encryption.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки, доктор фізико-математичних наук,
доктор юридичних наук, професор

КОЗІН ОЛЕКСАНДР БОРИСОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки,
кандидат фізико-математичних наук, доцент

ПАПКОВСЬКА ОЛЬГА БОРИСІВНА

Одеський національний політехнічний університет,
доцент кафедри вищої математики та моделювання систем,
кандидат фізико-математичних наук, доцент

РИЗИКИ: ПРАВОВА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Із багатьох публікацій у вітчизняних та іноземних виданнях відомо безліч визначень ризику, що несуть досить широке його тлумачення. Так, тільки у Інтернет-словниках міститься сотні тлумачень ризику у багатьох сферах людської діяльності (див. [1]). В наслідок цього виникають різні неоднозначності, пов'язані з розкриттям сутності самого ризику та пов'язаних з ним понять. Це стосується як технічної, так і юридичної сфери. Ризик має досить широке трактування. При цьому його соціальна сутність полягає перш за все в тому, що суб'єкт, свідомо відступаючи від встановлених в суспільстві правил поведінки, створює конфліктну ситуацію, загострює до межі проблему і, використовуючи переваги екстремальної ситуації, намагається вирішити поставлене завдання. Тому зрозумілим стають ймовірні ризики від непрофесійних керівників, які вважають себе «ефективними менеджерами». Відповідно такий стан характерний також і для сфери інформаційної безпеки та кібернетики, яка в даний час впроваджена в будь-яку систему управління. В зв'язку з цим, аналіз і розкриття поняття ризику для його