

Затверджено наказом
в.о. директора
Самбірського
фахового коледжу
економіки
та інформаційних
технологій
_____Марія САРАХМАН
Наказ № 90 від 08.06.2023

ІНСТРУКЦІЯ ЩОДО ВИКОРИСТАННЯ ОНЛАЙН СЕРВІСІВ

1. Загальні положення

1.1. Інструкція з використання онлайн сервісів розроблена відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», затвердженого постановою Кабінету Міністрів України від 19.06.2019 № 518; доручення Прем'єр-міністра України Дениса Шмигала № 2692/1/1-23 від 07.02.2023 до листа Головнокомандувача Збройних Сил України від 27.01.2023 № 300/1/C/672 щодо розробки інструкції з використання застосунків «Viber», «Telegram», «WhatsApp», «Facebook Messenger», «Google Messenger», «Apple iMessenger», «Microsoft Teams», «Microsoft Skype», «Signal», «Threma», «Wire», «Session», «Cisco Webex» та «Zoom» для обміну текстовими повідомленнями, проведення аудіо- та відеоконференцій в операційних системах Unix (IOS, Android) та Windows.

1.2. Враховуючи зазначене, онлайн сервіси відеоконференцій та програмні додатки загального призначення, такі як «Viber», «Telegram», «WhatsApp», «Facebook Messenger», «Google Messenger», «Apple iMessenger», «Microsoft Teams», «Microsoft Skype», «Signal», «Threma», «Wire», «Session», «Cisco Webex» та «Zoom» тощо не можуть використовуватись на обладнанні та робочих місцях, які входять до складу об'єкта критичної інформаційної інфраструктури.

Обробка державних інформаційних ресурсів або інформації з обмеженим

доступом, вимога щодо захисту якої встановлена законом повинна здійснюватися відповідно до вимог Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Так, відповідно до ст. 2 зазначеного закону об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

2. Вимоги безпеки

2.1. Для офіційного документообігу та ділової кореспонденції використовувати тільки електронну пошту коледжу.

2.2. Категорично заборонити використання застосунків: Viber і Telegram для передачі інформації з обмеженим доступом та проведення конференцій і відеозустрічей.

2.3. Для проведення конференцій, форумів, онлайн зустрічей та інших заходів використовувати Google сервіси: Class room і Meet які мають різні запобіжні заходи для збереження конфіденційності та безпеки даних.

2.4. Під час проведення аудіо- та відеоконференцій слід дотримуватись наступних заходів безпеки:

- підготувати середовище для роботи та переконатись, що в полі зору вебкамери не має жодних конфіденційних даних;
- увімкнути функцію шифрування аудіо- та відеозв'язку;
- не поширювати посилання на конференції у відкритому доступі та встановити пароль для входу, який необхідно змінювати для кожної нової сесії;
- контролювати підключення учасників;
- під час спільного використання екрану поширювати лише необхідні

- дані;
- налаштувати безпечну передачу файлів, для чутливих даних додатково налаштувати шифрування та парольний захист.

2.5. При використанні особистих електронних пристроїв для підключення до відкритих каналів зв'язку здійснити наступні налаштування:

- заборонити автоматичне встановлення додатків з невідомих джерел;
- обмежити доступ додатків до функціоналу пристрою, в якому немає потреби;
- відключити функцію автоматичного підключення до незахищених точок доступу.

3. Вибір оптимальних параметрів захисту

Адміністратори:

- *Підготувати мережу.* Дізнатися, як забезпечити високу якість відеозустрічі.
- *Налаштувати дозволи для здобувачів освіти та викладачів.* Надавати дозволи на створення, запис та трансляції відеозустрічі лише тим організаційним підрозділам до яких входять викладачі та співробітники.
- *Забезпечити захист відеозустрічі.* Якщо дозволено підключення по телефонній мережі загального користування, до відеозустрічі можуть приєднатися будь які учасники, які мають номер для підключення та PIN-код зустрічі. Щоб підвищити безпеку зустрічей заборонити з'єднання телефонної мережі.
- *Відслідковування показників якості проведення зустрічей.* Для забезпечення якості проведення зустрічей використовувати інструменти оцінки якості зв'язку в Meet

Викладачі:

- *Зробити початкові відеозустрічі недоступні для повторного використання учасниками.* Щоб здобувачі освіти не могли приєднуватися до зустрічі після її завершення необхідно створити відеозустріч із псевдонімами, а не запускати їх із заходу Google Календаря. Навіть якщо при використанні того самого псевдоніму

здобувачі освіти не зможуть повторно приєднатися до такої зустрічі після того, як її залишить останній учасник і 10-значний код перестане діяти.

- Відеозустріч із псевдонімом можна створити одним із наступних способів:
 - Перейти на сайт meet.google.com або відкрити мобільний додаток Meet та ввести псевдонім зустрічі у полі «Приєднатися до зустрічі або створити свою».
 - Використати код Meet, автоматично створений у Google Класі.

Куратори груп:

Пояснити здобувачам освіти про наступне.

- Перш ніж публікувати світлини або відео Мережі, слід отримати згоду людей які там зображені. Пам'ятати про недоторканість приватного життя особи.
- Не можна повідомляти свої паролі доступу друзям та знайомим. В загальнодоступному профілі краще використовувати деперсоніфіковані зображення, як фотографії профілю і вказувати мінімум персональної інформації, такої як вік, заклад освіти та місце проживання.
- Слід ділитись тільки тією інформацією, яку на їхню думку, дозволено побачити стороннім. Не слід ділитись інформацією, що дозволяє встановити їхню особистість або особистість інших.
- Здобувачі освіти повинні розуміти ризики пов'язані з використанням камер та опублікуванням контенту.

Всі учасники освітнього процесу, викладачі та здобувачі освіти повинні з повагою ставитися один до одного, адже безпека як очного так і дистанційного навчання залежить від педагогів, батьків та здобувачів освіти.

РОЗРОБИВ

Інженер комп'ютерних мереж

_____ Андрій САМАРДАК

УЗГОДЖЕНО

Завідувачка навчальної лабораторії
інформаційних і комунікаційних
технологій

_____ Оксана БУЦА