МІНІСТЕРСТВО ОСВІТИ ІНАУКИ УКРАЇНИ

Новороздільський політехнічний фаховий коледж

ЗАТВЕРДЖУЮ
Директор коледжу
_____ Іван ДИДИШИН
«__06__» _____ 2023 р.

ІНСТРУКЦІЯ

ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ ОНЛАЙН-СЕРВІСІВ ТЕЛЕКОНФЕРЕНЦІЙ ТА МЕСЕНДЖЕРІВ У НОВОРОЗДІЛЬСЬКОМУ ПОЛІТЕХНІЧНОМУ ФАХОВОМУ КОЛЕДЖІ

М. Новий Розділ

2023

Вступ

Інформація в сучасному світі — це стратегічний ресурс. Спотворення інформації може призвести до серйозних наслідків. Отже, забезпечення інформаційної безпеки в Україні є дуже актуальною задачею.

Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий Верховною Радою України 5 жовтня 2017 року, визначає онлайн-безпеку (кібербезпеку) як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

В умовах воєнного часу питання інформаційної безпеки виходить на якісно новий рівень. З урахуванням того, що заклади освіти через безпекову ситуацію проводять велику кількість занять у дистанційному режимі, існує реальна можливість витоку конфіденційної інформації щодо місця розміщення, сфери на змісту навчальної діяльності освітнього закладу, а також персональних даних учасників освітнього процесу. Адже центри обробки даних найпопулярніших на сьогоднішній день сервісів відеоконференцій та месенджерів (Viber, Telegram, WhatsApp, Facebook Messenger, Google Meet, Microsoft Teams, Microsoft Skype, Zoom) знаходяться за межами України. Відповідно до вимог Закону України «Про захист інформації в інформаційно-комунікаційних системах», інформація з обмеженим доступом повинна оброблятись у тих центрах обробки даних, які пройшли Державну експертизу з боку служби Держспецзв'язку України. Очевидно, що для закордонних інформаційних ресурсів провести таку експертизу є проблематично.

Саме тому, важливо не тільки забезпечити належну якість освітнього процесу під час роботи в дистанційному режимі, а й дотримуватись правил конфіденційності, безпеки та захисту персональних даних усіх учасників освітнього процесу. Саме з цією метою і була розроблена дана Інструкція.

1. Основні терміни та їх визначення

Терміни та визначення, зазначені у даній інструкції, подані відповідно до чинного законодавства України, зокрема згідно Законів України «Про інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та інших нормативно-правових документів, виданих органами державної влади України. Зокрема це:

Інформація - відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

Інформація з обмеженим доступом – це така інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову.

Конфіденційною є інформація про фізичну особу (освіта, сімейний стан, релігійність, стан здоров'я, дату і місце народження, майновий стан та інші

персональні дані), а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Службовою інформацією є інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, а також інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Месенджер - телекомунікаційна служба для обміну текстовими повідомленнями між комп'ютерами або іншими пристроями користувачів через комп'ютерні мережі.

Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Телекомунікації - передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

Телеконференція – вид заходу, в якому групова комунікація здійснюється між територіально розподіленими учасниками за допомогою технічних засобів.

2. Основні правила безпечної роботи з месенджерами та системами телеконференцій

1. Перед запуском конференції та увімкненням відеокамери переконайтесь, що в межах кута її огляду немає жодних об'єктів місцевості, документів, предметів та інших елементів, які містять ознаки інформації з обмеженим доступом. Найкраще під час проведення відеоконференції повністю «розмити» задній фон поза обличчям людини. Інструкція, як це зробити в Google Meet є тут: *https://support.google.com/meet/answer/10058482?hl=uk&co=GENIE.Platform%3DDesktop* , для Zoom тут: *http://surl.li/hwyzj*
2. Під час проведення конференції необхідно контролювати підключення учасників, не допускаючи до неї сторонніх осіб. Для цього рекомендується виконувати голосову ідентифікацію-привітання для кожної нової особи, яка приєднується до онлайн-заняття, а також змінювати посилання на конференцію для кожного нового онлайн-заняття.
3. Перед увімкненням режиму трансляції зображення з екрану монітора необхідно переконатись, що на Вашому комп'ютері не відкрито жодних програм та вкладок, які містять інформацію з обмеженим доступом, а також на робочому столі немає жодних файлів, назви та вміст яких містять інформацію з обмеженим доступом.

4. У разі потреби передачі через месенджери інформації, яка містить персональні дані учасників освітнього процесу (наприклад даних про результати контрольних заходів), необхідно попередньо зашифрувати її за допомогою спеціальних програм для шифрування документів, які використовують алгоритми шифрування та ключі електронного цифрового підпису, що відповідають Державним стандартам України. Зокрема це ПЗ **UmCa** від Державної казначейської служби України (*https://ca.treasury.gov.ua/)* або **PrivateSign** від АТ КБ «Приватбанк» (*https://acsk.privatbank.ua/main)*.

5. Після завершення роботи з месенджером чи сервісом онлайн-конференцій слід переконатись, що відповідна програма повністю завершила свою роботу і не працює у фоновому режимі. В іншому випадку слід примусово завершити її роботу, натиснувши правою кнопкою миші на зображення-емблему програми в області сповіщень панелі задач ОС Windows (біля годинника) та вибрати опцію завершення роботи чи виходу з програми. Якщо Вам необхідно, щоб месенджер працював у фоновому режимі постійно (наприклад з метою обміну повідомленнями зі студентами в режимі реального часу), то слід переконатись, що під час роботи месенджера у фоновому режимі на комп'ютері не проводиться обробка інформації з обмеженим доступом.

3. Під час роботи з месенджерами та системами телеконференцій ЗАБОРОНЕНО:

1. Передавати інформацію з обмеженим доступом у будь-якому вигляді (як візуально, так і у вигляді електронних файлів) в месенджерах та сервісах відеоконференцій, які не мають експертних висновків щодо механізмів захисту інформації з боку Держспецзв'язку України. У разі необхідності щодо передачі такої інформації слід користуватись серверами електронної пошти, центр обробки даних яких знаходиться в Україні (ukr.net, meta.ua тощо) або месенджері «Розмова», а також попередньо зашифрувати цю інформацію з використанням ключа електронного цифрового підпису за допомогою спеціалізованого програмного забезпечення (див. пункт 4 розділу 2 даної Інструкції).

2. Залишати працювати у фоновому режимі програми-месенджери та системи телеконференцій на комп'ютерах, які виконують обробку інформації з обмеженим доступом (бухгалтерія, відділ кадрів, канцелярія, адміністратор ЄДеБО, приймальна комісія тощо). У разі наявності потреби щодо використання месенджерів чи сервісів телеконференцій на таких комп'ютерах, необхідно попередньо закрити усі програми та прибрати з робочого столу усі файли, які містять інформацію з обмеженим доступом.