«ЗАТВЕРДЖУЮ»
В.о. ректора ВНЗ «ПрАТ «ЛІМ»
_____ В. М. Миронюк
від «08» червня 2023 р.

ВНУТРІШНЯ ІНСТРУКЦІЯ
з використання онлайн сервісів у освітній діяльності
ВНЗ «ПрАТ «Львівський інститут менеджменту»

1. Ця Інструкція розроблена у відповідності до: доручення Віце-прем'єрміністра з інновацій, розвитку освіти, науки та технологій — Міністра цифрової трансформації від 14.04.2023 № 2692/14/1-23 Щодо використання онлайн сервісів відео-конференцій та програмних додатків загального призначення; розпоряджень Департаменту освіти і науки Львівської обласної військової адміністрації: від 30.05.2023 №21-1222/0/2-23 Щодо використання онлайн сервісів; від 30.05.2023 №21-1224/0/2-23 Щодо використовуваного програмного забезпечення.

2. Ця Інструкція визначає єдині вимоги щодо:

– умов, правил і процедур використання в освітній діяльності ВНЗ «ПрАТ «Львівський інститут менеджменту» таких застосунків, як «Viber», «Telegram», «WhatsApp», «Facebook Messenger», «Google Messenger», «Apple IMessenger»,«Microsoft Teams», «Microsoft Skype», «Signal»,«Threema», «Wire», «Session», «Cisco Webex» та «Zoom»;

– недопущення використання в освітній діяльності ВНЗ «ПрАТ «Львівський інститут менеджменту» шкідливого програмного забезпечення, програмних продуктів чи технічних рішень, що мають російське походження та/або створені підприємствами, які афілійовані з країною агресором.

3. Усім учасникам освітнього процесу при використанні зазначених застосунків:

3.1. В обов'язковому порядку заборонено передачу інформації з обмеженим доступом.

3.2. Рекомендується дотримуватись основних правил кібергігієни, саме:

– використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте;

– користуйтеся антивірусним програмним забезпеченням із технологією евристичного аналізу;

– використовуйте програмний міжмережевий екран (брандмауер) і штатні засоби захисту від шкідливого програмного забезпечення;

– здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи»;

– не підключайте флешки та зовнішні диски, не вставляйте CD і DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо ви знайшли пристрій всередині офісу або на вулиці, чи отримали його поштою або з доставкою, чи незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити та перевірити його вміст – є велика ймовірність, що пристрій є небезпечним;

– довіряйте лише власним пристроям та будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях

– при підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення

– відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf)

– не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте стійкі паролі, зокрема такі що: містять не менше 8 символів; містять літери, цифри та спеціальні символи; не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів і серій документів, автотранспорту, банківської картки, адреси реєстрації тощо); не використовуються в будь-яких інших аккаунтах;

– уникайте використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях);

– будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. На сьогодні найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів і не відкривати файли навіть з безпечними розширеннями. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, усе одно потрібно перевірити (у телефонному режимі або в будь-який інший спосіб), чи дійсно ця особа відправляла вам повідомлення з вкладенням;

– іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами. Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Зважайте, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим;

– будьте особливо пильними при користування Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми), не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви, зазвичай, не відвідуєте;

– будьте уважними до проявів Інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі Інтернет є фішинг. Особливу увагу варто звертати на доменне

ім'я Інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо). В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані;

– у разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат веб-сайту, щоб переконатися, що він не клонований або не підроблений;

– шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами на кшталт tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.

– використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів;

– будьте обережні щодо спливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не «схвалюйте» і не «приймайте» нічого похапцем;

– під час використання віддаленого доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting);

– установіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій;

– слідкуйте за новинами про нові кіберзагрози та швидко реагуйте на нові виклики.

4. Усім учасникам освітнього процесу під час проведення аудіо- та відеоконференцій слід суворо дотримуватись таких заходів безпеки:

– підготувати середовище для роботи та переконатись, що в полі зору веб камери не має жодних конфіденційних даних і таких, що мають безпосереднє чи опосередковане відношення до питань обороноздатності країни;

– увімкнути функцію шифрування аудіо- та відео зв'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, а для «чутливих» даних додатково налаштувати шифрування та парольний захист;

5. Усім учасникам освітнього процесу при використанні особистих електронних пристроїв для підключення до відкритих каналів зв'язку, рекомендується зробити такі налаштування:

– заборонити автоматичне встановлення додатків із невідомих джерел;

– обмежити доступ додатків до функціоналу пристрою, в якому немає потреби;

– відключити функцію автоматичного підключення до незахищених точок доступу.