

Висновок. Отже, можна зробити висновок що медіатор відіграє ключову роль у формуванні здорової корпоративної культури та врегулювання конфлікту. Його діяльність не обмежується лише на вирішення існуючих суперечках, в має значно ширший характер. Таким чином залучення медіатора стає стратегічним інструментом для побудови здорових відносин між персоналом, де конфлікт розцінюється не як загроза, а як можливість для розвитку і самовдосконалення, довіри та підвищення загальної ефективності команди.

Список використаних джерел:

1. Дзевелюк М.В., Дзевелюк А.В. Особливості використання медіації у підготовці юристів та публічних службовців в зво. Медіація & Університети 1.0: Матеріали Міжнар. наук.-практ.конф. 15 лист. 2024р., Чернівці: 2024. С. 113-117.
2. Медіація у професійній діяльності юриста : підручник / ред. Н. Крестовська, Л. Романадзе ; Українська академія медіації. Одеса : Екологія, 2019. 462 с. ISBN 978-617-7046-89-8.
3. Дзевелюк М.В. Медіація як інструмент модернізації системи органів державної влади та органів місцевого самоврядування в Україні. Наукові перспективи. Вип. № 6(60) 2025. С. 111-122.

УДК 347

Максимук Олександр

Здобувач вищої освіти факультету права, публічного управління і менеджменту

Вінницького державного педагогічного університету імені Махайла

Коцюбинського

Скічко Ірина

доктор філософії, асистент кафедри публічно-правових дисциплін Вінницького

державного педагогічного університету

імені Михайла Коцюбинського

ОСВІТА ТА КІБЕРБЕЗПЕКА

Ключові слова: кібербезпека, освіта, інтернет-джерела, інтернет-ресурс, освітній заклад.

Актуальність. Сьогодні освіта та її подача є неможливою без використання електронних ресурсів, однак вони можуть бути як корисними для нас так і шкідливими, збиваючи нас з пантелику недостовірною інформацією. Ризики відносно роботи з інтернет-джерелами можуть бути різними, це може бути не тільки дезінформація, але й активна участь зловмисника через веб-сторінку з якою взаємодіє студент чи засобами комунікації, до прикладу соц-мережі. А тому маючи на сьогоднішній день дану проблему, варто знати стратегію захисту.

Для початку вкажемо конкретніше які існують загрози кібербезпеки в освіті: Завантаження навчальних матеріалів із неперевіраних та недостовірних ресурсів; Фішинг - це той вид шахрайства коли зловмисники шляхом обману змушують вас розкрити різного роду конфіденційної інформації; DDoS-атаки - це кібератака яка може здійснюватись із кількох пристроїв, задля перезавантаження та блокування сервера. Що в результаті буде часткове або повністю виведене із ладу інтернет-ресурс [1].

Варто зазначити, що шкідливий контент та кібербулінг є постійними проблемами які активно починають виникати у шкільний період і може залишатись до моменту навчання у вищих навчальних закладах. Таким проблемам варто приділити увагу саме тоді коли вони починають з'являтися у підлітка чи зрілої людини. Найнебезпечніший вплив йде на підлітків, адже вони можуть сприймати це по своєму і найбільші наслідки переживатиме саме це покоління. Їх характер може змінюватись а самооцінка знижуватись. Задля подолання такої проблеми викладачам слід проводити бесіди на такі теми, мати такі стосунки із учнями, аби вони могли звернутись до викладача, як до друга, тим самим створюючи безпечне середовище [2].

Отож, коли ми знаємо з чим боримось ми можемо вивести стратегію захисту. Для початку слід оцінити ризики. Надалі варто відразу відокремити цінну інформацію на вашому пристрої та захистити її в першу чергу. Після захисту усіх даних, потрібно зрозуміти які наявні слабкі місця у нашому середовищі та переглянути існуючий захист, тобто ми пересвідчуємось чи він буде працювати і що необхідно чекати у разі інциденту. В загальному існують певні правила безпечного зберігання даних, і їх варто розглянути більш детальніше. Для початку звернемо увагу на класичне резервне копіювання даних. Варто регулярно використовувати таку функцію, задля відновлення видалених чи пошкоджених даних. Обов'язково слід оновлювати програмне забезпечення, особливу увагу варто приділити антивірусам. Чим старіше програмне забезпечення – тим більший шанс у зловмисника отримати ваші дані. Також варто мати обмежений доступ до конфіденційних даних учнів, студентів, викладчів та співробітників закладу. Певна інформація, така як особисті дані повинні мати обмежений доступ та/або доступні тільки для співробітників безпеки. Використання шифрування ваших даних для захисту інформації тобто паролів є основою. Фактично саме це ми можемо спостерігати у наших власних телефонах, адже ми хочемо зберегти власну інформацію від осіб, так само слід захищати і дані закладу. Сам доступ до мережі закладу повинні мати багатофакторну автентифікацію, задля кращого захисту. Це метод авторизації, коли особа повинна підтвердити що це справді вона через надання декількох доказів. Наприклад наш комп'ютер чи мережа інтернету інколи може нас перевіряти що це ми показуючи на вибір картинки чи вводячи нарисований код це і є автентифікація. Для кращого захисту, слід обрати відповідальну уповноважену особу. Заклад повинен призначити ту особу, яка буде слідкувати за інформаційним простором та безпекою щодо мережі та даних закладу. Вона повинна вчасно реагувати на інциденти, проводити регулярну перевірку та інші заходи безпеки [1].

Висновки. Таким чином, захистом даних мають займатись не тільки студенти та учні навчального закладу, але й викладачі та його співробітники.

Адже саме вони створюють той інформаційний простір для здобувачів освіти, який має бути достовірним. Захист даних є важливим фактором для доцільного навчання студентів та учнів. І тому не варто нехтувати банальними правилами безпеки, встановивши пароль чи зробивши резервне копіювання даних, а краще зайнятись більш серйозно захистом даних. Звичайний вірус чи одна атака шахраїв може легко прибавити роботу працівникам освітнього закладу та заплутати усіх учасників навчального процесу, що в результаті і призупинить саме навчання. Це є частиною нас і майбутнє стає теперішнім.

Список використаних джерел:

1. Забезпечення кібербезпеки в освітніх установах: обізнаність, правила, стратегія. 07.02.25. URL: <https://osvitafp.com.ua/2025/02/07/zabezpechennia-kiberbezpeky-v-osvitnikh-ustanovakh-obiznanist-pravyla-stratehiia/> (дата звернення 24.09.2025).
2. Кібербезпека в освіті. URL: <https://www.pdau.edu.ua/sites/default/files/node/4518/pravylaoformlennyaspyskuvykorystanyhdzherel.pdf> (дата звернення 26.09.2025).

УДК 658.012

Марич Маргарита

Здобувачка вищої освіти факультету права, публічного управління і менеджменту

Вінницького державного педагогічного університету імені Михайла Коцюбинського

Науковий керівник: Зубар Іван, кандидат економічних наук,
старший викладач кафедри публічного управління та менеджменту
факультету права, публічного управління і менеджменту
Вінницького державного педагогічного університету
імені Михайла Коцюбинського