Методичні рекомендації щодо кібербезпеки в освітніх закладах

1. Використовувати виключно ліцензійне програмне забезпечення та забезпечувати його своєчасне оновлення.
2. Забезпечити використання антивірусного програмного забезпечення з актуальними антивірусними базами, а також організувати регулярне проведення повної перевірки систем на предмет наявності шкідливого програмного забезпечення.
3. У разі виявлення ознак зараження негайно від’єднувати інфіковані сервери та робочі станції від локальної обчислювальної мережі до повного усунення загрози.
4. Під час отримання повідомлень електронною поштою, у випадку якщо ім’я або адреса відправника, а також зміст повідомлення викликають підозру, не відкривати вкладені файли та не переходити за наданими посиланнями.
5. Налаштувати фільтрування вхідних та вихідних інформаційних потоків, зокрема шляхом заборони отримання працівниками електронних повідомлень, що містять у вкладеннях виконувані файли.
6. Налаштувати та використовувати механізми SPF, DKIM та DMARC для зменшення кількості спаму, протидії підміні відправника (spoofing) та інших видів кібератак.
7. Обмежити права доступу користувачів, заборонивши ініціалізацію та запуск файлів з правами адміністратора без відповідного обґрунтування.
8. Для роботи з сервісами електронної пошти використовувати виключно поштові клієнти або офіційні вебінтерфейси, рекомендовані адміністратором системи.
9. Політики інформаційної безпеки закладів освіти повинні передбачати обмеження використання знімних носіїв інформації (флеш-накопичувачів), у тому числі обов’язкову їх перевірку антивірусним програмним забезпеченням.
10. Заборонити або відключити стандартні сервіси шифрування операційної системи, що не використовуються у службовій діяльності, з метою унеможливлення їх використання шкідливим програмним забезпеченням типу «шифрувальник».
11. Обмежити можливість запуску виконуваних файлів (*.exe, *.js, *.com, *.bat, *.jar, *.vbs тощо) з каталогів Temp, AppData та інших тимчасових директорій.
12. Заборонити або суттєво обмежити використання макросів у програмному забезпеченні Microsoft Office.
13. Обмежити або заборонити використання середовища PowerShell, окрім випадків, коли його застосування є обґрунтованим та контрольованим.
14. На регулярній основі забезпечити створення резервних копій програмного забезпечення та критично важливих даних з їх зберіганням на відокремлених, захищених ресурсах.

15. Забезпечити обов’язкову зміну всіх стандартних (заводських) логінів і паролів доступу до систем відеоспостереження, маршрутизаторів та іншого мережевого обладнання у закладах освіти.

16. Забезпечити регулярне оновлення програмного забезпечення та прошивок камер відеоспостереження й мережевого обладнання.

17. Встановити складні унікальні паролі доступу (не менше 10–12 символів із використанням літер різного регістру, цифр та спеціальних символів).

18. Запровадити обов’язкову періодичну зміну паролів доступу до систем відеоспостереження та іншого мережевого обладнання не рідше одного разу на 60–90 днів, а також у кожному випадку зміни відповідальних осіб або виникнення підозри щодо компрометації облікових даних.

19. Обмежити віддалений доступ до систем відеоспостереження, дозволивши його виключно з визначених IP-адрес або через захищені VPN-з’єднання.

20. Організувати проведення інструктажів та роз’яснювальної роботи з керівниками закладів освіти та відповідальними працівниками щодо основ кібергігієни та ризиків використання незахищених технічних засобів.

21. У разі виявлення фактів несанкціонованого доступу, підозрілої активності або ознак кібератаки негайно інформувати правоохоронні органи з метою реагування та фіксації інциденту.