Додаток
до Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій (пункт 10)

Орієнтовний перелік
навчальних тем для проведення інструктажів і тренінгів щодо кібергігієни

1. Основи кібергігієни

1.1. Визначення основних понять у сфері кібербезпеки, кібергігієни, цифрової грамотності.
1.2. Види вразливостей та загроз у кіберпросторі (шкідливе ПЗ, фішинг, соціальна інженерія, витік даних тощо).
1.3. Основні принципи безпечної поведінки в цифровому середовищі (кіберпросторі).
1.4. Наслідки порушення правил кібергігієни.

2. Захист облікових записів та авторизаційних (автентифікаційних) даних

2.1. Парольна безпека, правила створення паролів, їх менеджмент.
2.2. Ризики повторного використання паролів та їх безпечне зберігання.
2.3. Використання двофакторної (2FA) або багатофакторної (MFA) автентифікації.

3. Захист кінцевого (термінального) обладнання

3.1. Оновлення (актуалізація) операційних систем і програмного забезпечення.
3.2. Використання антивірусів, антишпигунських програм і фаєрволів.
3.3. Методи захисту кінцевого (термінального) обладнання (PIN, біометрія, шифрування).
3.4. Фізична безпека кінцевого (термінального) обладнання (екранні фільтри, блокування інтерфейсу, безпечне використання та зберігання).

4. Безпека електронної пошти та повідомлень

4.1. Розпізнавання фішингових листів і вкладень.
4.2. Безпечне поводження з підозрілими листами.
4.3. Цифровий підпис і шифрування листування.
4.4. Захист корпоративної пошти.

5. Соціальна інженерія

5.1. Основні методи маніпуляцій (pretexting, baiting, tailgating тощо).
5.2. Типові приклади атак на довіру.

5.3. Правила верифікації осіб і запитів.
5.4. Симуляція атак соціальної інженерії.

6. Безпечне користування мережею Інтернет
6.1. Захищене з'єднання (HTTPS, VPN).
6.2. Безпека під час роботи у публічних WI-FI мережах.
6.3. Блокування реклами, шкідливих скриптів, трекерів.
6.4. Загрози, пов'язані із завантаженням файлів з невідомих джерел.

7. Захист персональних даних
7.1. Основи законодавства про захист персональних даних (GDPR, Закон України «Про захист персональних даних»).
7.2. Мінімізація цифрового сліду.
7.3. Безпечне публікування інформації в соцмережах.
7.4. Обробка, передача та зберігання конфіденційної інформації.

8. Соціальні мережі та месенджери
8.1. Приватність і налаштування доступу.
8.2. Загрози при спілкуванні з невідомими особами.
8.3. Ризики поширення фейків та маніпулятивного контенту.
8.4. Безпечне використання Telegram, WhatsApp, Signal, Facebook, Instagram тощо.

9. Поведінка під час кіберінцидентів
9.1. Ознаки виникнення кіберінцидентів, кібератак.
9.2. Порядок дій при підозрі на зараження або витік.
9.3. Кому повідомляти: внутрішні канали та зовнішні служби (CERT-UA).
9.4. Підготовка до кризових ситуацій (створення резервних копій, план відновлення).

10. Робота з корпоративними системами
10.1. Політики безпечного доступу до інформаційно-комунікаційних систем.
10.2. Поводження з внутрішніми системами/сервісами та документами.
10.3. Логування дій користувачів.
10.4. Робота з інформацією з обмеженим доступом.

11. Віддалена робота та кібергігієна
11.1. Безпека при використанні персональних пристроїв (BYOD).
11.2. Безпечна організація домашнього офісу.
11.3. VPN і тунелювання з'єднання.
11.4. Ризики під час відеоконференцій.

12. Профілактичні заходи та навчання
12.1. Культура кібергігієни на робочому місці.
12.2. Рольова модель безпечної поведінки.
12.3. Оцінка ризиків і самостійний аудит.

12.4. Регулярне навчання, тестування знань та сертифікація.

13. Додаткові теми

13.1. Штучний інтелект і конфіденційність.
13.2. Фейкові новини, дезінформація, кіберпропаганда.
13.3. Інтернет речей (IoT) та нові виклики безпеки.

_____