ПОЛТАВСЬКИЙ РЕГІОНАЛЬНИЙ ЦЕНТР ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ «Основи кібергігієни»

Шифр програми: ЗК/2021/12

Рік запровадження програми: 2021

Програму затверджено: Протокол засідання навчально-методичної ради

від 14 вересня 2021 року № 3

Програму погоджено :наказ НАДС від 23 жовтня 2021року № 172-21

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація	
Назва програми	Основи кібергігієни
Шифр програми	ЗК/2021/12
Тип програми за змістом	загальна короткострокова програма підвищення кваліфікації
Форма навчання	змішана (дистанційно-очна)
Цільова група	державні службовці категорії «Б», «В, посадові особи місцевого самоврядування
Передумови навчання за програмою	
Найменування замовника освітніх послуг у сфері професійного навчання за програмою	Полтавська обласна державна адміністрація Полтавська обласна рада Місцеві ради
Найменування партнера (партнерів) програми	Координатор проектів ОБСЄ в Україні у рамках проекту ««Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки». Швейцарсько-український проєкт «Підтримка децентралізації в Україні» DESPRO. Національна онлайн платформа «Дія. Цифрова освіта» Міністерства цифрової трансформації України
Обсяг програми	1 кредит ЄКТС
Тривалість програми та організація навчання	до двох тижнів навчання дистанційно в асинхронному режимі та два дні очно
Мова(и) викладання	українська
Напрям(и) підвищення кваліфікації, який (які) охоплює програма	кібербезпека
Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму	цифрова грамотність; робота з інформацією
Укладач(і) програми	Глєбова Алла Олександрівна, доцент кафедри публічного управління, адміністрування та права Національного університету «Полтавська політехніка імені Юрія Кондратюка», сертифікований тренер УШУ з кібергігієни alliaglebova@gmail.com Манжай Олександр Володимирович, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент, національний спеціаліст проектів Координатора проектів ОБСЄ в Україні, moj@univd.kharkov.ua Іщенко Тетяна Михайлівна, кандидат

	економічних наук, начальник управління програм підвищення кваліфікації Тренінгового центру УШУ, tishchenko@usg.org.ua
2. Загальна мета	
підвищення рівня професійної компетентності щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в державному органі / органі місцевого самоврядування	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
знання	основних положень та термінів, що стосуються кібергігієни на робочу місці; основної нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки; заходів кібергігієни на робочої місці; особливостей кібергігієни в системі публічної служби
уміння	визначати заходи кібергігієни для конкретної ситуації; оцінювати загрози та вживати заходів реагування на робочому місці;
навички	організації безпечного доступу до пристроїв і програм; правильного налаштування програмного забезпечення на робочому місці; критичного оцінювання інформації
4. Викладання та навчання(методи навчання, форми проведення навчальних занять)	
Дистанційна частина в асинхронному режимі передбачає проходження учасниками професійного навчання онлайн курсу (перегляд відеолекцій, інформаційних матеріалів, опрацювання обов'язкової літератури, виконання тестових та іншого виду завдань). Очна частина передбачає участь учасників професійного навчання у дводенному тренінгу.	
5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься дистанційне навчання із зазначенням посилання (вебадреси)	навчання в асинхронному режимі (теми 1- 9): Дія. Цифрова освіта https://osvita.diia.gov.ua/; Спільнота практик: сталий розвиток https://udl.despro.org.ua/
Назва дистанційного курсу (модуля)	Основи кібергігієни
6. Оцінювання і форми поточного, підсумкового контролю	
Критерії оцінювання та їх питома вага у підсумковій оцінці (%)	Відвідування занять – 30 % Проходження дистанційного навчання – 30 % Поточний контроль – 10 % Підсумковий контроль – 30 % Документ про підвищення кваліфікації видається за умови набрання учасником професійного навчання не менше ніж 75 %, обрахованих з урахуванням питомої ваги кожного із критеріїв оцінювання
Форма підсумкового контролю	електронне тестування

СТРУКТУРА ПРОГРАМИ

Назва теми	Кількість годин				
	загальна кількість годин / кредитів ЄКТС	у тому числі:			
		аудиторні заняття	дистанційні заняття	навчальні візити	самостійна робота слухачів
1	2	3	4	5	6
Тема 1. Соціальна інженерія	1,5		1		0,5
Тема 2. Безпечне користування мережею Інтернет	1,5		1		0,5
Тема 3. Безпечне користування електронною поштою	1,5		1		0,5
Тема 4. Шкідливе програмне забезпечення	1,5		1		0,5
Тема 5. Безпека користування соціальними мережами	1,5		1		0,5
Тема 6. Безпека мобільних пристроїв	1,5		1		0,5
Тема 7 Фізична безпека	1,5		1		0,5
Тема 8. Убезпечення від неправдивих повідомлень	1,5		1		0,5
Тема 9. Правові засади кібергігієни	2		1		1
Тема 10. Практикум «Основи кібергігієни»	15	15			
Підсумковий контроль результатів навчання	1	1			
РАЗОМ	**30 / 1**	**16**	**9**		**5**

ЗМІСТ ПРОГРАМИ

Тема 1. Соціальна інженерія

Поняття соціальної інженерії. Причини та умови соціальної інженерії. Прийоми, методи та принципи соціальної інженерії. Психологія впливу та загальні рекомендації для органів публічної влади.

Тема2. Безпечне користування мережею Інтернет

Браузер та його функції. Доменні імена. Шифрування комунікацій. Організація авторизації в Інтернеті з використанням браузера. Безпечне використання плагінів. Рекомендації з убезпечення браузеру. Безпечне користування мережами Wi-Fi. Відповідальне оприлюднення інформації.

Тема 3. Безпечне користування електронною поштою

Розмежування використання особистої та службової поштових скриньок. Загрози під

час користування поштовою скринькою. Аналіз листів, що містять ознаки фішінгу. Рекомендації щодо захисту електронної пошти. План дій на випадок компрометації пошти.

Тема 4. Шкідливе програмне забезпечення

Загрози для програмного забезпечення. Оновлення програмного забезпечення. Ліцензійне та неліцензійне програмне забезпечення. Типи шкідливого програмного забезпечення. План дій у випадку зараження інформаційної системи. Загальні рекомендації з використання програмного забезпечення.

Тема 5. Безпека користування соціальними мережами

Соціальні мережі: загальні положення. Безпечна реєстрація в соціальних мережах. Налаштування конфіденційності та інших питань безпеки. Шахрайство в соціальних мережах. Відповідальне розповсюдження інформації у соціальних мережах. Рекомендації з безпечної роботи в соціальних мережах.

Тема 6. Безпека мобільних пристроїв

Правила обмеження доступу до мобільних пристроїв. Безпечна робота в мультимедійних засобах спілкування. Особливості передавання вживаних мобільних пристроїв іншим особам. Особливості передавання контактної інформації іншим особам. Головні загрози, які виникають під час роботи з мобільними пристроями. Основні правила безпечної роботи з мобільними пристроями.

Тема 7. Фізична безпека

Роль фізичної безпеки у кіберзахисті організації. Безпека контрольованої зони. Загрози, які виникають під час використання змінних носії інформації. Рекомендації щодо фізичної безпеки.

Тема 8. Убезпечення від неправдивих повідомлень

Види маніпуляцій з інформацією у кіберсфері. Пропаганда як інструмент інформаційного впливу. Заходи протидії неправдивим повідомленням.

Тема 9. Правові засади кібергігієни

Кібербезпека та інформаційна безпека як елементи національної безпеки України. Основні елементи стратегії кібербезпеки України. Співвідношення понять кібербезпека та кібергігієна. Основні пріоритети забезпечення інформаційної безпеки. Види інформації за порядком доступу. Захист відкритої інформації. Особливості захисту інформації з обмеженим доступом.

Тема 10. Практикум «Основи кібергігієни»

Встановлення інформації про володільця доменного імені та IP-адреси. Безпечні комунікації в мережі Інтернет. Фішінг. Налаштування антивірусу. Пошук інформації в соціальних мережах. Облікові записи, які використовуються в мобільних пристроях. Рольова гра з фізичної безпеки. Аналіз достовірності інформації.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Документ (сертифікат) про підвищення кваліфікації учаснику навчання видається за умови:

проходження дистанційної частини курсу в асинхронному режимі, що є передумовою допуску до участі у практичних заняттях (частка виконання програми – 40 % у т. ч. поточний контроль);

участі у тренінгу в очному форматі (частка виконання програми – 30 %);

успішного проходження підсумкового контролю у формі тестування (частка виконання програми – 30 %).

Учасник (учасниця) професійного навчання, який (яка) виконав (виконала) програму в обсязі не менше 75% обрахованих з урахуванням питомої ваги кожного із критеріїв оцінювання та за умови успішного проходження підсумкового контролю отримає сертифікат про підвищення кваліфікації.

ЛІТЕРАТУРА, ІНФОРМАЦІЙНІ РЕСУРСИ, ОБОВ'ЯЗКОВІ ДЛЯ ОПРАЦЮВАННЯ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI.URL:https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
5. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл.
6. Кевін Митник. «Мистецтво залишатись непоміченим. Хто ще читає ваші імейли?», «Наш формат». 2019. 280с.