Програма заходу БПР
«Кібергігієна та кіберзахист в медичній сфері:
Безпека даних та медичних систем»

Вид заходу: **тренінг**
Дата проведення: **03 лютого 2026 року**
Час початку: **10:00**

Погодинний виклад змісту заходу:

ЧАС	ЗМІСТ	ВИКОНАВЦІ
09.45 - 10.00	Реєстрація учасників.	Ірина ГОЛОВІНА, завідувачка тренінгового центру
10.00 – 10:15	**Частина 1: Вступ до кібербезпеки в медицині** Вітальне слово. Оголошення регламенту роботи. Представлення мети заходу, важливості теми для медичної галузі	Ігор МАТКОВСЬКИЙ, генеральний директор ДУ «Вінницький ОЦКПХ МОЗ» Галина МОХНІЙ, заступник генерального директора ДУ «Вінницький ОЦКПХ МОЗ»
10:15– 10:45	**"Чому кібербезпека важлива для медиків?"** ***Лекція-презентація*** – Огляд сучасних кіберзагроз (віруси-вимагачі, фішинг, шпигунське ПЗ). – Специфіка кіберзагроз для медичної сфери (витік даних пацієнтів, кіберсаботаж медичного обладнання, вплив на безперервність лікування). – Юридичні та етичні аспекти захисту медичних даних (GDPR, HIPAA, українське законодавство). – Приклади реальних кібератак на медичні заклади.	Наталія КУЗНЄЦОВА, Начальник відділу інформаційних систем та захисту інформації
11:00 - 11:30	**Практичний кейс.** Наслідки кіберінцидентів для медичної практики та репутації клініки.	Наталія КУЗНЄЦОВА,
11:30 – 12:00	**Частина 2: Основи кібергігієни для кожного медика** "Паролі та багатофакторна аутентифікація – ваш перший рубіж захисту." ***Лекція-презентація*** – Принципи створення надійних паролів (довжина, складність, унікальність). – Використання менеджерів паролів. – Що таке багатофакторна аутентифікація (MFA) і чому її потрібно використовувати скрізь.	Дмитро ГРИГОРЕНКО, фахівець з організації інформаційної безпеки
12:00- 12:30	**"Розпізнавання фішингу та соціальної інженерії."** ***Лекція-презентація*** – Ознаки фішингових листів, SMS, дзвінків. – Типові схеми соціальної інженерії, спрямовані на медиків. – Як перевіряти посилання та вкладення.	Дмитро ГРИГОРЕНКО, фахівець з організації інформаційної безпеки

	– Практикум: Аналіз прикладів реальних фішингових листів, вправа "Знайди ознаки фішингу". – Візуалізація: "Шлях фішингової атаки".	
12:30 12:45	Перерва	
12:45- 13:45	**<u>Ботоферми, фейкові новини та цифровий слід: як захистити репутацію та не стати жертвою маніпуляцій."</u>** – **Ботоферми та інформаційні операції:** ***Лекція-презентація*** o Що таке ботоферми, як вони функціонують і які цілі переслідують (дискредитація, поширення дезінформації, маніпуляція громадською думкою). o Як відрізнити реальних користувачів від ботів у соціальних мережах та коментарях. o Вплив дезінформації на медичну сферу (антивакцинаторство, псевдонаукові "ліки", паніка). o Репутаційні ризики для медичних закладів та лікарів від цілеспрямованих кампаній ботоферм.	Наталія КУЗНЄЦОВА,
	– **Цифровий слід:** ***Лекція-презентація*** o Що таке цифровий слід (активний та пасивний). o Важливість контролю за особистою інформацією, яка поширюється в мережі. o Як мінімізувати свій цифровий слід, особливо у професійному контексті. o Конфіденційність медичних працівників та пацієнтів у соціальних мережах.	Наталія КУЗНЄЦОВА,
13:45- 14:15	**<u>Частина 3: Безпечне поводження з даними та пристроями</u>** **"Безпека робочих станцій та мобільних пристроїв."** ***Лекція-презентація*** – Оновлення програмного забезпечення (операційна система, антивірус, медичні програми). – Використання ліцензійного ПЗ. – Безпечне використання USB-накопичувачів та інших зовнішніх носіїв. – Ризики використання особистих пристроїв (BYOD) в робочих цілях. – Захист від втрати та крадіжки пристроїв (шифрування, віддалене блокування).	Дмитро ГРИГОРЕНКО,
14:15- 14:45	**Безпечна робота з електронними медичними картками та інформаційними системами."** ***Лекція-презентація*** – Принципи мінімального доступу (кожен бачить лише те, що потрібно для роботи). – Важливість виходу з облікового запису після завершення роботи. – Передача медичних даних: безпечні канали зв'язку, шифрування.	Наталія КУЗНЄЦОВА,

14:45-15-00	Практичний розбір: Обговорення ситуацій з неправомірним доступом до даних ЕМК.	Всі учасники
15:00-15:20	**Частина 4: Реагування на кіберінциденти та майбутнє** **"Що робити у разі підозри на кіберінцидент?"** ***Лекція - презентація*** – Алгоритм дій: кому повідомляти (ІТ-відділ, керівництво), що фіксувати. – Важливість негайного реагування. – Не намагатися вирішити проблему самостійно (якщо ви не ІТ-спеціаліст). – План відновлення після атаки (резервне копіювання).	Дмитро ГРИГОРЕНКО,
15:20-15:45	Підсумкове оцінювання набутих знань та практичних навичок	Всі учасники
15:45 – 16:05	Підведення підсумків. Обговорення і рефлексія з визначенням успіхів та досягнень кожного з учасників; фідбек.	Всі учасники

Астрономічних годин – **6**
Академічних годин – **8**.