

Програма проведення заходу

Вид заходу: тренінг

Тема заходу: «Кібергігієна та кіберзахист в медичній сфері: безпека даних та медичних систем»

Дата проведення: 27 жовтня 2026 року

Точна адреса проведення (детально) / Посилання на захід, для здійснення моніторингового візиту (при потребі, будь ласка, використовуйте пошту bpr@testcentr.org.ua або bpr.monitoring@gmail.com): вул. Князів Коріатовичів, 185, місто Вінниця, Вінницька область, Україна. Військово-медичний клінічний центр Центрального регіону

ПІБ та номер телефону контактної особи, яка відповідає за реєстрацію заходу та подання результатів проведення: Головіна Ірина Сергіївна, +380674306306

ПІБ та номер телефону контактної особи, яка відповідає за проведення (є на місці проведення): Головіна Ірина Сергіївна, +380674306306

Кількість астрономічних годин:(перерви понад 15 хв не враховуються): 8

Кількість навчальних (академічних) годин: (кількість астрономічних годин *60/45): 10

час початку 10:00 <i>погодинний виклад змісту заходу (1. Вступ (привітання, знайомство, ознайомлення з метою, очікуваннями, регламентом). 2. Теоретичний блок (представлення ключових понять, технік, технологій, лекція, презентація або відеоматеріал, питання-відповіді). 3. Практична частина (робота в групах, кейс-аналіз, симуляції, групові обговорення, презентація результатів роботи учасників). 4. Рефлексія та підведення підсумків, оцінювання набутих знань)</i> час завершення 18:00		ПІБ викладача/тренера/доповідача, місце роботи, посада
9:45 – 10:00	Реєстрація учасників заходу	Ірина ГОЛОВІНА, завідувач тренінгового центру ДУ «Вінницький ОЦКПХ МОЗ»
10:00 – 10:15	Вітальне слово, ознайомлення з метою, очікуваннями, регламентом. Початок заходу	Ігор МАТКОВСЬКИЙ, генеральний директор ДУ «Вінницький ОЦКПХ МОЗ»
10:15– 10:45	"Чому кібербезпека важлива для медиків?" - 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).	Наталія КУЗНЄЦОВА, Начальник відділу інформаційних систем та захисту інформації

	• Приклади реальних кібератак на медичні заклади.	
10:45 -11:30	Практичний кейс. Наслідки кіберінцидентів для медичної практики та репутації клініки.	Наталія КУЗНЄЦОВА,
11:30 –12:15	Основи кібергігієни для кожного медика "Паролі та багатофакторна аутентифікація – ваш перший рубіж захисту." • 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
12:15-12:45	"Розпізнавання фішингу та соціальної інженерії." • Ознаки фішингових листів, SMS, дзвінків. • Типові схеми соціальної інженерії, спрямовані на медиків. • Як перевіряти посилання та вкладення.	Дмитро ГРИГОРЕНКО,
12:45-13:15	• Практикум: Аналіз прикладів реальних фішингових листів, вправа "Знайди ознаки фішингу". • Візуалізація: "Шлях фішингової атаки".	Дмитро ГРИГОРЕНКО,
13:15 - 13:30	Перерва	
13:30-14:00	<u>Ботоферми, фейкові новини та цифровий слід: як захистити репутацію та не стати жертвою маніпуляцій"</u> • Ботоферми та інформаційні операції: ○ Що таке ботоферми, як вони функціонують і які цілі переслідують (дискредитація, поширення дезінформації, маніпуляція громадською думкою). ○ Як відрізнити реальних користувачів від ботів у соціальних мережах та коментарях. ○ Вплив дезінформації на медичну сферу (антивакцинаторство, псевдонаукові "ліки", паніка). ○ Репутаційні ризики для медичних закладів та лікарів від цілеспрямованих кампаній ботоферм.	Наталія КУЗНЄЦОВА,
14:00-14:30	Цифровий слід (практична вправа): ○ Що таке цифровий слід (активний та пасивний).	Наталія КУЗНЄЦОВА,

	○ Важливість контролю за особистою інформацією, яка поширюється в мережі. ○ Як мінімізувати свій цифровий слід, особливо у професійному контексті. ○ Конфіденційність медичних працівників та пацієнтів у соціальних мережах.	
14:30-15:15	<u>Безпечне поводження з даними та пристроями</u> "Безпека робочих станцій та мобільних пристроїв." – 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,
15:15-16:00	Безпечна робота з електронними медичними картками та інформаційними системами" • 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,
16:00-16:45	Практичний розбір: Обговорення ситуацій з неправомірним доступом до даних ЕМК.	Всі учасники
16:45-17:30	Реагування на кіберінциденти та майбутнє (практична вправа) "Що робити у разі підозри на кіберінцидент?" • 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,
17:30-18:00	Рефлексія та підведення підсумків, оцінювання набутих знань	Всі учасники
18:00	Завершення заходу	