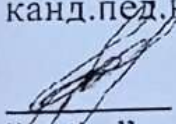


Чортківський медичний фаховий коледж

ЗАТВЕРДЖУЮ
Заступник директора
з навчальної роботи
канд.пед.наук


Христина КОЗАК
"13" "11" 2025 року

Протокол № 4 від 13.11.2025

НАВЧАЛЬНА ПРОГРАМА

заходу безперервного професійного розвитку
працівників сфери охорони здоров'я

ЗАГАЛЬНА ЦИФРОВА ГРАМОТНІСТЬ ПРАЦІВНИКІВ ОХОРОНИ ЗДОРОВ'Я.

ЗАХІД БПР
працівників сфери охорони здоров'я

1.	Назва заходу БПР	Загальна цифрова грамотність працівників охорони здоров'я.
2.	Цільова аудиторія (відповідно до Номенклатури спеціальності)	Медичні працівники з числа фахівців у сфері охорони здоров'я медсестринського профілю (акушерська справа, анестезіологія та реанімація, екстрена медицина, загальна практика-сімейна медицина, організація і управління охороною здоров'я, лікувальна справа, педіатрія, психіатрія, сестринська справа, хірургія, рентгенологія, травматологія і ортопедія, фізична та реабілітаційна медицина), стоматологічні спеціальності (стоматологія), спеціальності фармацевтичного профілю (фармація)
3.	Мета заходу	<ul style="list-style-type: none"> - розвиток цифрових компетентностей для роботи з електронною системою охорони здоров'я (ЕСОЗ) як екосистемою інформаційних відносин всіх учасників медичного середовища, що базуються на економічно ефективному та безпечному використанні інформаційно-комунікаційних технологій, спрямованих на підтримку системи охорони здоров'я, включаючи медичні послуги, профілактичний нагляд за здоров'ям, медичну літературу та медичну освіту, знання та дослідження - підвищити рівень цифрової грамотності працівників сфери охорони здоров'я шляхом формування і вдосконалення ефективних сучасних цифрових практичних навичок, необхідних для ефективного використання інформаційно-комунікаційних технологій у професійній діяльності - систематизувати та поглибити теоретичні знання у сфері ІТ-технологій, підвищити рівень загальної цифрової грамотності шляхом формування практичних навичок роботи з текстовим, табличним та презентаційним програмним забезпеченням, - розвиток вміння критично оцінювати інформацію під час пошуку в інтернеті та розпізнавати ознаки онлайн-шахрайства і

		<p>маніпуляцій.</p> <ul style="list-style-type: none"> - сприяти оволодінню правилами ефективної цифрової комунікації та мережевого етикету - забезпечити розуміння принципів кібербезпеки й дотримання вимог щодо захисту персональних даних пацієнтів. - забезпечити здатність медичних фахівців безпечно та результативно застосовувати цифрові інструменти для роботи з електронними медичними даними, комунікації з пацієнтами та колегами, організації клінічних процесів, а також для дотримання стандартів кібербезпеки й конфіденційності медичної інформації. - надати комплексне уявлення про права пацієнтів щодо захисту їх персональних та медичних даних, про відповідальність медичних працівників у забезпеченні цих прав, а також сформувати базові навички роботи з цифровими технологіями ЕСОЗ з точки зору забезпечення захисту персональних даних пацієнтів - поглибити знання про лікарську таємницю, розглянути правові основи захисту лікарської таємниці, порядок її розкриття та наслідки неправомірного розголошення лікарської таємниці - підготовка медичних фахівців до безпечного, етичного та результативного використання цифрових технологій у професійній діяльності.
4.	Перелік компетентностей, що набуваються або вдосконалюються	<ol style="list-style-type: none"> 1. Інформаційно-цифрова компетентність Здатність ефективно працювати з цифровою інформацією: здійснювати пошук, оцінювання достовірності, впорядкування та безпечне використання даних у професійній діяльності. Володіння базовими інструментами для роботи з електронними ресурсами, медичними інформаційними системами та цифровим контентом. 2. Компетентність у роботі з офісним програмним забезпеченням та онлайн-інструментами Уміння працювати з базовими офісними

		<p>програмами, сервісами для підготовки презентацій, таблиць, документів, календарів, а також хмарними сховищами й іншими сервісами, корисними в медичній практиці та адмініструванні.</p> <p>Здатність ефективно використовувати текстові редактори, табличні процесори та програмне забезпечення для створення презентацій з метою підготовки медичної документації, аналітичних матеріалів, освітніх та інформаційних матеріалів. Уміння застосовувати основні та розширені функції цих інструментів у професійній діяльності.</p> <p>3. Інформаційно-аналітична компетентність</p> <p>Уміння здійснювати пошук інформації в інтернеті з критичним оцінюванням її достовірності, надійності джерел та потенційних ризиків маніпуляції. Здатність відрізнити фейки, дезінформацію й упереджений контент, застосовуючи інструменти цифрової верифікації.</p> <p>4. Компетентність у сфері кібербезпеки та захисту даних</p> <p>Знання принципів безпечної роботи та поведінки в цифровому середовищі, включаючи розпізнавання шахрайських схем, фішингових атак, соціальної інженерії, захист персональних медичних даних, управління паролями, виявлення кіберзагроз, дотримання нормативних вимог щодо конфіденційності та інформаційної безпеки. Розуміння ризиків і способів їх мінімізації. Здатність виконувати базові та розширені заходи кібербезпеки з метою захисту власних пристроїв, професійних облікових записів і доступу до медичних даних. Розуміння принципів конфіденційності, нормативних вимог щодо захисту персональних медичних даних та правил їх обробки в цифрових системах. Здатність забезпечувати безпечно зберігання, передачу й використання інформації про пацієнтів відповідно до етичних і правових стандартів.</p> <p>5. Навички цифрової етики</p> <p>Усвідомлення етичних аспектів використання цифрових технологій у</p>
--	--	---

		<p>медицині, включаючи відповідальне поведження з інформацією, дотримання прав пацієнтів, регуляторних норм і професійних стандартів. Поглиблення знань щодо принципів медичної етики і деонтології для захисту конфіденційної інформації про пацієнта. Уміння ефективно та етично спілкуватися в цифровому середовищі: вести електронне листування, працювати в професійних онлайн-платформах, користуватися сервісами для дистанційної взаємодії. Дотримання норм мережевого етикету, поваги до колег і пацієнтів, коректного професійного спілкування.</p> <p>6. Цифрова самостійність і навчання впродовж життя</p> <p>Здатність самостійно опановувати нові цифрові інструменти, адаптуватися до технологічних змін, застосовувати цифрові ресурси для підвищення ефективності роботи та власного професійного розвитку.</p>
5.	Опис структури заходу	<p>Модуль1: Основи цифрової грамотності та робота з текстовими документами</p> <p><i>Тема1.1:</i> Поняття цифрової грамотності та цифрового середовища медичного працівника: компетентності, потреби, ризику.</p> <p><i>Тема1.2:</i> Основи роботи з комп'ютером і хмарними сервісами (файлова структура, формати файлів, збереження й обмін документами).</p> <p><i>Тема1.3:</i> Робота з текстовим програмним забезпеченням (створення медичної документації та інформаційних матеріалів, форматування медичної інформації, застосування стилів, шаблонів, списків, колонтитулів, редагування та рецензування тексту, коментарі, вставка таблиць, зображень, схем, складання інструкцій, інформаційних листів та коротких звітів.</p> <p>Модуль2: Табличне та презентаційне програмне забезпечення</p> <p><i>Тема2.1:</i> Табличні процесори(навігація та структура таблиць, формати даних, базові формули: сума, середнє, мінімум/максимум,</p>

обчислення показників, сортування, фільтрування, умовне форматування, побудова простих діаграм для аналізу медичних даних, представлення даних.

Тема 2.2 Презентаційне програмне забезпечення (принципи візуальної грамотності та медичної комунікації, структура ефективної презентації (мета, логіка, візуальні акценти), використання шаблонів, інфографіки, діаграм, фото та відео, основи дизайну: баланс тексту та зображень, контраст, доступність для аудиторії, підготовка професійних презентацій, аналітичне опрацювання базових даних.

Модуль 3: Цифрова безпека: захист від кіберзагроз, шахрайства та маніпуляцій

Тема 3.1: Основи кібербезпеки для медичного працівника (критичне оцінювання достовірності джерел та контенту, методи виявлення фейків, дезінформації та маніпуляцій, розпізнавання фішингу, соціальної інженерії, шахрайських схем, небезпечних посилань та фейкових сайтів, цифрові інструменти фактчекінгу та перевірки надійності інформації)

Тема 3.2: Практики безпечної роботи в інтернеті, захист пристроїв і робочих акаунтів (складні паролі, менеджери паролів, двофакторна автентифікація, захист пристроїв, безпечні мережі та підключення, поради з мінімізації ризиків та дій у разі підозрілих цифрових інцидентів, алгоритм дій при підозрі на кібератаку або витік даних)

Модуль 4. Цифрове спілкування, мережевий етикет та захист персональних даних пацієнтів

Тема 4.1: Мережевий етикет: культура взаємодії, професійний стиль спілкування, уникнення конфліктів (правила професійної цифрової комунікації, етикет електронної пошти, етичні норми поведінки в онлайн-середовищі, онлайн-платформи, відео конференції, робота з медичними платформами та відеозв'язком.)

		<p><i>Тема 4.2: Захист персональних даних пацієнтів: коректне зберігання, передавання й обробка медичної інформації (правові й етичні принципи конфіденційності в медицині, захист персональних даних пацієнтів: правила зберігання, передавання, обмеження доступу, роль кіберігієни при роботі з чутливою інформацією, загрози кібербезпеці персональних даних, порядок дій при витоку даних та при неправомірному доступі третіх осіб до персональних даних пацієнта.</i></p>
6.	Загальний обсяг навчального навантаження	Кількість астрономічних годин/академічних годин – 7,5/10
7.	Форми організації та проведення заходу	Лекції, мультимедійні презентації, практична робота (відпрацювання практичних навичок), оцінювання знань (тестування). Обговорення практичних кейсів, ситуаційний аналіз, пояснення, дискусія.
8.	Методи організації та проведення заходу	Словесний, тренувальний, аналітичний, ситуаційний аналіз.
9.	Матеріально-технічне забезпечення заходу	Комп'ютер для презентацій та відео
10.	Форма підсумкового контролю	Тестування (20 тестових та ситуаційних завдань). Для успішного проходження тестування слухач повинен правильно відповісти на 60% запитань (12 правильних відповідей). Зараховане тестування позначається як виконав, не зараховане – не виконав.