

1.1. Політика безпеки (далі - Політика) є стратегічним документом, що визначає комплекс заходів, спрямованих на гарантування фізичного захисту, ментального благополуччя, цифрової захищеності та створення безбар'єрного простору для всіх учасників проєкту ERASMUS+ Jean Monnet Module «European Regulation of the Cryptocurrency Market: Implementation in Ukraine» (далі - ERCM). Ця Політика базується на фундаментальній вимозі програми Erasmus+ щодо забезпечення захисту, здоров'я та безпеки учасників, яка гарантує право кожної особи навчатися та розвиватися у безпечному середовищі, що поважає її фізичну та емоційну недоторканність.

1.2. Реалізація проєкту на базі Національного юридичного університету імені Ярослава Мудрого у місті Харкові відбувається в умовах безпрецедентних викликів, пов'язаних із повномасштабною збройною агресією проти України. Політика інтегрує механізми мітигації воєнних, епідеміологічних та організаційних ризиків із зобов'язаннями щодо підтримки інклюзії та екологічної сталості, створюючи цілісну екосистему стійкості (resilience) освітнього процесу.

2. Управління фізичною безпекою в умовах кризових загроз

2.1. Найвищий пріоритет Політики безпеки - збереження життя та здоров'я учасників проєкту. Враховуючи високу ймовірність та критичний рівень впливу воєнних загроз у регіоні розташування Університету, робоча група впроваджує жорсткі протоколи реагування на надзвичайні ситуації.

2.2. Основним превентивним заходом є радикальна гнучкість форматів проведення заходів. За замовчуванням більшість навчальних модулів, вебінарів проводяться в онлайн або змішаному форматі.

2.3. У разі проведення очних зустрічей організатори зобов'язані завчасно ознайомити учасників із планами евакуації та розташуванням найближчих укриттів цивільного захисту. У разі оголошення повітряної тривоги будь-який захід негайно призупиняється, а всі присутні спускаються до укриття, де за можливості може бути продовжена комунікація.

2.4. Політика передбачає протокол релокації: у разі критичного загострення безпекової ситуації в Харкові ключові процеси адміністрування проєкту, документація та частина викладацького складу можуть бути переміщені у більш безпечні регіони України або за кордон, що забезпечує безперервність виконання грантової угоди.

2.5. Окрім воєнних ризиків, Політика враховує санітарно-епідеміологічні загрози. За потреби передбачається оперативний перехід на дистанційний формат, забезпечення дезінфекційних заходів, контроль вентиляції та готовність до повної цифровізації навчального процесу.

3. Психологічна безпека, інклюзивність та розмаїття

3.1. Безпека в межах програми Erasmus+ охоплює також ментальне здоров'я та інклюзивну культуру (Inclusion and Diversity).

3.2. У проєкті впроваджується політика нульової толерантності до булінгу, харасменту, мови ворожнечі та будь-яких форм психологічного тиску під час академічних взаємодій.

3.3. Викладачі забезпечують підтримувальне середовище (trauma-informed approach), у якому кожен учасник має право на помилку та заохочується до вільного висловлення думок.

3.4. Враховуючи енергетичні та безпекові виклики, встановлюються гнучкі дедлайни, а всі лекції записуються для асинхронного доступу.

3.5. Особлива увага приділяється інклюзивності для осіб з інвалідністю, внутрішньо переміщених осіб та учасників з обмеженим доступом до інтернету. Матеріали адаптуються до

вимог цифрової доступності, забезпечується менторський супровід. Відсутність фінансового бар'єра гарантується безкоштовною участю у проєкті.

4. Цифрова безпека (Cybersecurity)

4.1. Захист віртуального середовища забезпечується через використання ліцензованих платформ для відеоконференцій із належними налаштуваннями безпеки та захистом від несанкціонованого доступу.

4.2. Верифікація учасників є обов'язковою умовою доступу до онлайн-заходів і навчальних матеріалів.

4.3. Учасники отримують інструктаж із кібербезпеки щодо створення надійних паролів, захисту акаунтів та розпізнавання фішингових атак.

5. Екологічна сталість та Green Erasmus

5.1. Політика безпеки інтегрує принципи екологічної сталості та вимоги Green Erasmus.

5.2. Проєкт впроваджує безпаперовий документообіг із повним переходом на електронні матеріали.

5.3. Використання дистанційного навчання та віртуальної мобільності дозволяє суттєво зменшити вуглецевий слід і транспортні викиди.

5.4. Усі організаційні рішення ухвалюються з урахуванням впливу на екологічну сталість.

6. Управління ризиками та безпековими загрозами

6.1. Політика передбачає системний підхід до управління ризиками, визначеними на етапі планування проєкту:

6.1.1. Ескалація збройного конфлікту: передбачено перехід на дистанційне навчання, евакуацію персоналу та релокацію активностей до безпечніших партнерських ЗВО.

6.1.2. Енергетичні та комунікаційні збої: передбачено дублювання матеріалів у хмарних сервісах, запис занять та гнучкість дедлайнів.

6.1.3. Комунікаційні бар'єри та зниження залученості: застосовується комунікаційний план і регулярне анкетування учасників для коригування контенту.

6.1.4. Епідеміологічні обмеження: передбачено дотримання рекомендацій МОЗ та оперативний перехід на дистанційні формати навчання.

6.2. Моніторинг виконання Політики є безперервним процесом, за який відповідають усі члени робочої групи. Усі інциденти фіксуються та за потреби узгоджуються з грантодавцем відповідно до процедур реалізації проєкту.