

ЗМІСТ

ЛАБОРАТОРНА РОБОТА № 1. ДОСЛІДЖЕННЯ АТАК УХИЛЕННЯ ВІД ЗМАГАЛЬНОСТІ НА МОДЕЛІ МАШИННОГО НАВЧАННЯ НА ОСНОВІ SUPPORT VECTOR MACHINE (SVM)	7
ВКАЗІВКИ З ПІДГОТОВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ.	7
ТЕОРЕТИЧНІ ВІДОМОСТІ	8
ПРИКЛАДИ ПРАКТИЧНИХ ЗАВДАНЬ.....	13
ЗАГАЛЬНЕ ЗАВДАННЯ ДЛЯ ВИКОНАННЯ.....	23
КОНТРОЛЬНІ ПИТАННЯ.....	23
ЛАБОРАТОРНА РОБОТА № 2. ДОСЛІДЖЕННЯ ПЕРЕНОСИМОСТІ АТАК УХИЛЕННЯ	25
ВКАЗІВКИ З ПІДГОТОВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ.	25
ТЕОРЕТИЧНІ ВІДОМОСТІ	26
ПРИКЛАДИ ПРАКТИЧНИХ ЗАВДАНЬ.....	33
ЗАГАЛЬНЕ ЗАВДАННЯ ДЛЯ ВИКОНАННЯ.....	49
КОНТРОЛЬНІ ПИТАННЯ.....	50
ЛАБОРАТОРНА РОБОТА № 3. ДОСЛІДЖЕННЯ АТАК ОТРУЄННЯ (POISONING ATTACKS) НА МОДЕЛІ МАШИННОГО НАВЧАННЯ.	52
ВКАЗІВКИ З ПІДГОТОВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ.	52
ТЕОРЕТИЧНІ ВІДОМОСТІ	53
ПРИКЛАДИ ПРАКТИЧНИХ ЗАВДАНЬ.....	56
ЗАГАЛЬНЕ ЗАВДАННЯ ДЛЯ ВИКОНАННЯ.....	71
КОНТРОЛЬНІ ПИТАННЯ.....	71
ЛАБОРАТОРНА РОБОТА № 4. ДОСЛІДЖЕННЯ ВИКОНАННЯ АТАК УХИЛЕННЯ ТА ОТРУЄННЯ НА НАБОРІ ДАНИХ MNIST.....	73
ВКАЗІВКИ З ПІДГОТОВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ.	73
ТЕОРЕТИЧНІ ВІДОМОСТІ	74

ПРИКЛАДИ ПРАКТИЧНИХ ЗАВДАНЬ.....	76
ЗАГАЛЬНЕ ЗАВДАННЯ ДЛЯ ВИКОНАННЯ.....	89
КОНТРОЛЬНІ ПИТАННЯ.....	90
ЛАБОРАТОРНА РОБОТА № 5. ДОСЛІДЖЕННЯ АТАКИ УХИЛЕННЯ (EVASION ATTACKS) НА НЕЙРОННІ МЕРЕЖІ З ВИКОРИСТАННЯМ НАБОРУ ДАНИХ MNIST	91
ВКАЗІВКИ З ПІДГОТОВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ.	91
ТЕОРЕТИЧНІ ВІДОМОСТІ	92
ПРИКЛАДИ ПРАКТИЧНИХ ЗАВДАНЬ.....	93
ЗАГАЛЬНЕ ЗАВДАННЯ ДЛЯ ВИКОНАННЯ.....	106
КОНТРОЛЬНІ ПИТАННЯ.....	107
СПИСОК ЛІТЕРАТУРИ.....	108