ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«МЕТІНВЕСТ ПОЛІТЕХНІКА»

РОБОЧА ПРОГРАМА
навчальної дисципліни

«ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Затверджено на засіданні кафедри
цифрових технологій та проєктно-
аналітичних рішень
Протокол № 1 від 02.09.2025 р.

Запоріжжя 2025

metinvest polytechnic

УКЛАДАЧІ:

Шматко Олександр, к.т.н, доцент, доцент кафедри цифрових технологій та програмно-аналітичних рішень;
Кондратов Олексій, старший викладач кафедри цифрових технологій та програмно-аналітичних рішень.

УЗГОДЖЕНО:

Гарант освітньої програми
«Комп'ютерні науки» Ірина ГЕТЬМАН

ЗАТВЕРДЖЕНО

Завідувач кафедри Ірина СМИРНОВА

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Опис курсу. Основи кібербезпеки та захисту інформації – обов'язкова навчальна дисципліна, яка забезпечить багатоаспектний розгляд поняття захисту інформації в інформаційних системах з позицій інтересів користувачів, програмістів, операторів, експлуатаційників, адміністраторів комп'ютерних мереж та обчислювальних систем. Мета викладання дисципліни полягає в навчанні сучасним технологіям захисту даних в інформаційних системах та мережах, а також створення систем комплексного захисту інформації в установі, де розгортається інформаційна мережа.

Особливістю курсу є акцент на: нормативно-правові основи організації інформаційної безпеки; основні загрози інформаційній безпеці, правила їх виявлення, аналізу та визначення вимог до різних рівнів забезпечення інформаційної безпеки; загрози інформаційній безпеці, створювані комп'ютерними вірусами, вивчення особливостей цих загроз та характерних рис комп'ютерних вірусів; вивчення особливостей забезпечення інформаційної безпеки в комп'ютерних мережах і специфіки засобів захисту комп'ютерних мереж а також основні прийоми захисту корпоративних мереж при використанні Internet.

Отримані знання будуть корисними для вирішення проблем забезпечення відмово стійкості та безпеки в інформаційних системах, що прямо пов'язані з питаннями забезпечення їх інформаційної захищеності в першу чергу від кібератак.

Вимоги:

– базові знання з алгоритмізації та програмування, схемотехніки та архітектури комп'ютерів, системного аналізу, комп'ютерних мереж;

– математичні знання та навички з диференціального та інтегрального обчислень, функцій багатьох змінних;

– наявність корпоративного облікового запису @mipolytech.education, Microsoft Teams, Word, Excel;

– наявність особистого логіну та паролю в Moodle (для отримання або поновлення слід звернутися до відповідальної особи на факультеті).

Програмні результати навчання.

– володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп’ютерних систем, знати мережні технології, архітектури комп’ютерних мереж, мати практичні навички технології адміністрування комп’ютерних мереж та їх програмного забезпечення;

– розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати

безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Організація курсу, форми та методи навчання.

Освітній процес будується як комбінація лекцій та самостійного вивчення навчального матеріалу на платформі Moodle – з одного боку, та практичних занять з опануванням навичок розв’язання задач захисту інформаційних (комп'ютерних) мереж та систем через їх моделювання та оцінки результатів роботи – з іншого.

Практичні заняття передбачають розбір теоретичних та практичних питань з вивчення способів та засобів проєктування, розробки та моделювання корпоративних комп'ютерних (інформаційних) мереж, а також вивчення критеріїв, методів та засобів забезпечення інформаційної безпеки та шляхи запобігання комп’ютерним інцидентам з ураженням інформації з застосуванням програмного забезпечення Virtual Box.

Окрім роботи на практичних заняттях здобувачу необхідно буде виконати індивідуальне завдання та модульні контрольні роботи у терміни, встановлені у розділі «Розподіл балів за контрольними точками та графік їх виконання».

З урахуванням поточної ситуації від учасників освітнього процесу очікується виконання вимог безпеки при сигналі «Повітряна тривога», санкції за залишення заняття або неявку на заняття не застосовуються.

Опціонально доступні індивідуальні та групові консультації, які проводяться з метою допомоги студентам у виконанні їх самостійних завдань та роз’яснення окремих розділів теоретичного та практичного матеріалу. З викладачем можна зв’язатися через електронну пошту, в чаті або в персональній розмові в MS Teams.

Підсумковий контроль з даної дисципліни відбувається у формі іспиту.

Іспит виставляється лише по сукупності виконання контрольних точок та підсумкового тестового або розрахункового завдання.

Мова освітнього процесу: українська, англійська (окремі джерела літератури, фактологічна та інша інформація).

2 НАВЧАЛЬНА ПРОГРАМА

Змістовний модуль 1. Системний підхід та цілі кібербезпеки

Тема 1. Принципи забезпечення безпеки в комп'ютерних системах.

Поняття кібербезпеки та її місце в системі інформаційної безпеки. Системний підхід до забезпечення кібербезпеки. Основні цілі кібербезпеки: конфіденційність, цілісність, доступність. Інформаційні активи та загрози для них. Модель порушника та сценарії атак.

Тема 2. Віртуалізація як середовище для досліджень кібербезпеки.

Поняття віртуалізації та її роль у кібербезпеці. Типи віртуалізації: повна, паравіртуалізація, контейнеризація. Віртуальні машини як безпечне середовище для експериментів. Побудова навчальної лабораторії з використанням Kali Linux та Metasploitable. Мережева взаємодія віртуальних середовищ.

Тема 3. Основи мережевої безпеки

Архітектура комп'ютерних мереж. Типові мережеві вразливості.

Загрози мережевого рівня. Захист мережевих сервісів. Роль фаєрволів та сегментації мережі.

Тема 4. Аналіз та експлуатація вразливостей.

Поняття вразливості та експлойту. Класифікація вразливостей. Методи виявлення вразливостей. Експлуатація вразливостей у навчальному середовищі. Поняття бекдору та механізми його функціонування.

Змістовний модуль 2. Безпека віддаленого доступу та атаки перебором

Тема 5. Протокол SSH для захищеного управління.

Поняття віддаленого доступу. Загрози незахищеного керування системами. Протокол SSH: принципи роботи та архітектура.

Шифрування та автентифікація в SSH. Переваги використання SSH.

Тема 6. Адміністрування SSH у Kali Linux.

Налаштування SSH-сервера. Управління користувачами та правами доступу. Конфігураційні файли SSH. Типові помилки конфігурації. Практичні аспекти захисту SSH-з'єднань.

Тема 7. Криптографічна стійкість та ключі доступу.

Поняття криптографічної стійкості. Симетричне та асиметричне шифрування в SSH. Ключі доступу та їх генерація. Аутентифікація за допомогою ключів. Управління та захист криптографічних ключів.

Тема 8. Методологія атак Brute Force.

Поняття атаки перебором. Передумови успішності brute force-атак. Інструменти для реалізації атак перебором. Етапи виконання атаки brute force. Наслідки атак перебором для системи.

Змістовний модуль 3. Методи захисту та моніторинг

Тема 9. Різновиди атак методом перебору.

Онлайн та офлайн brute force-атаки. Словникові атаки. Гібридні атаки. Атаки з використанням списків витоків паролів. Особливості реалізації атак у мережевому середовищі.

Тема 10. Стійкість паролів та оцінювання часу злому.

Фактори стійкості паролів. Довжина та складність паролів. Методи оцінювання часу перебору. Вплив хешування та сольових значень. Практичний аналіз надійності паролів.

Тема 11. Превентивні заходи захисту.

Політики керування паролями. Обмеження кількості спроб входу.

CAPTCHA як механізм захисту. Двофакторна автентифікація (2FA). Комплексний підхід до запобігання атакам перебором.

Тема 12. Моніторинг інцидентів та аналіз журналів.

Поняття події та інциденту кібербезпеки. Журнали безпеки та їх призначення. Аналіз лог-файлів у Linux. Виявлення атак за журналами подій. Основи реагування на інциденти.

3 ОБСЯГ І СТРУКТУРА ДИСЦИПЛІНИ

Розподіл обсягу дисципліни за видами навчальних занять та темами для денної форми навчання для освітньої програми «Комп'ютерні науки», для якої вивчення дисципліни є обов'язковою

№ з/п	Назви змістових модулів і тем	Кількість годин				
		Усього	в т.ч.			
			Л	П (С)	Лаб	СРС
Змістовий модуль 1. Розгортання лабораторії та аналіз вразливостей						
1	Системний підхід та цілі кібербезпеки	11	1	2	0	8
2	Віртуалізація як середовище для досліджень	11	1	2	0	8
3	Мережева безпека.	11	1	2	0	8
4	Експлуатація вразливостей та бекдори	11	1	2	0	8
Змістовний модуль 2. Безпека віддаленого доступу та атаки перебором						
5	Протокол SSH для захищеного управління	12	2	4	0	6
6	Адміністрування SSH у Kali Linux	11	1	4	0	6
7	Криптографічна стійкість та ключі доступу	11	1	4	0	6
8	Методологія атак Brute Force	12	2	4	0	6
Змістовний модуль 3. Методи захисту та моніторинг						
9	Різновиди атак методом перебору	11	2	2	0	7
10	Фактори стійкості паролів та час злому	11	2	2	0	7
11	Превентивні заходи та двофакторна автентифікація	11	1	4	0	6
12	Моніторинг інцидентів та аналіз журналів	12	2	2	0	8
Усього годин		**135**	**17**	**34**	**0**	**84**

Тут і далі: Л – лекції, П (С) – практичні (семінарські) заняття, Лаб – лабораторні заняття, СРС – самостійна робота студентів.

Розподіл обсягу дисципліни за видами навчальних занять та темами для освітніх програм, в яких дисципліна є вибірковим компонентом.

№ з/п	Назви змістових модулів і тем	Кількість годин				
		Усього	в т.ч.			
			Л	П (С)	Лаб	СРС
Змістовий модуль 1. Розгортання лабораторії та аналіз вразливостей						
1	Системний підхід та цілі кібербезпеки	11	1	2	0	8
2	Віртуалізація як середовище для досліджень	11	1	2	0	8
3	Мережева безпека.	11	1	2	0	8
4	Експлуатація вразливостей та бекдори	11	1	2	0	8
Змістовний модуль 2. Безпека віддаленого доступу та атаки перебором						
5	Протокол SSH для захищеного управління	12	2	4	0	6
6	Адміністрування SSH у Kali Linux	11	1	4	0	6
7	Криптографічна стійкість та ключі доступу	11	1	4	0	6
8	Методологія атак Brute Force	12	2	4	0	6
Змістовний модуль 3. Методи захисту та моніторинг						
9	Різновиди атак методом перебору	11	2	2	0	7
10	Фактори стійкості паролів та час злому	11	2	2	0	7
11	Превентивні заходи та двофакторна автентифікація	11	1	4	0	6
12	Моніторинг інцидентів та аналіз журналів	12	2	2	0	8
Усього годин		**135**	**17**	**34**	**0**	**84**

4 ПІДХОДИ ДО ОЦІНЮВАННЯ

4.1 Розподіл балів за контрольними точками

Тижні / Види контр. точок	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Всього
Робота на практичних заняттях				10		10			10		10							40
Складання індивідуальних завдань							10					10				10		30
Модульні контрольні роботи								10					10				10	30
Всього	40								40					20				100

Дисципліна є вибірковим компонентом освітніх програм

Тижні / Види контр. точок	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Всього
Робота на практичних заняттях				10		10			10		10							40
Складання індивідуальних завдань							10					10				10		30
Модульні контрольні роботи								10					10				10	30
Всього	40								40					20				100

4.2 Зміст та вимоги до контрольних точок

Назва контрольної точки	Опис контрольної точки, порядок її проходження та отримання балів
ПР1. «Розгортання та налагодження віртуальної лабораторії Kali Linux». ПР2. «Дослідження та експлуатація бекдора у Metasploitable (навчальне середовище)». ПР3. «Конфігурація та захист SSH у Kali Linux». ПР4. «Дослідження інструментів Brute Force Attack та методів захисту».	Роботи ПР1…ПР4 виконуються та захищаються на аудиторних заняттях у межах практикуму з моделювання мереж (мах 10 балів за кожну). Протягом семестру надаються звіти із виконаних робіт, які прикріплюються в Мудлі. Оцінка за кожну виконану практичну роботу оголошується на занятті і може бути оскаржена. – студент дав пряму і релевантну відповідь на поставлене питання з використанням обґрунтованого посилання на теоретичний матеріал та варіації зміни відповіді на зміну вхідних умов, в т.ч. у вигляді додаткових запитань (5 бали); – оцінка ініціативності у роботі над завданням, логічності та структурованості відповіді, здатності комунікувати у команді та під впливом негативних факторів, в т.ч. під тиском викладача

Назва контрольної точки	Опис контрольної точки, порядок її проходження та отримання балів
	та/або групи, вміння вести дискусію та бути критичним та самокритичним (5 бали).
Виконання та захист індивідуальних завдань	Підготовлене есе у вигляді файлу *docx, або *pdf розміщується у відповідному розділі дисципліни в Moodle і перевіряється протягом тижня після завершення терміну подачі. Оскарження оцінки може бути здійснене на останньому практичному занятті поточного мудулю. Max 10 балів за одну роботу: – студент підготував есе за завданням, в якому: правильно визначив проблеми, комплекс факторів, які могли вплинути на їх виникнення, обґрунтував своє бачення теоретичними концепціями або моделями, виконав необхідні розрахунки в разі потреби, представив висновок або власне бачення виходу з проблеми і окреслив можливі перспективи і обмеженість такого рішення; есе структуровано, викладено діловим, науковим або публіцистичним стилем української (6 бали); – використання штучного інтелекту (ШІ) не забороняється, оскільки пропозиції відомих застосунків ШІ суттєво залежать від обміркованої постановки питання і уточнюючих питань; однак в разі, якщо відповідь, отримана з використанням ШІ, не є комплексною або не відповідає за стилем і викладеними позиціями іншим частинам есе або завдання, містить очевидно неправдиву інформацію, то оцінка за цим критерієм знижується (2 бал); – студент під час презентації / захисту есе демонструє володіння термінологічним апаратом, відповідає на запитання, здатний швидко адаптувати позицію під зміни у вихідному ситуаційному завданні (2 бал)
Модульні контрольні роботи	МКР виконуються в Moodle під час останнього практичного заняття в модулі за 1 годину 10 хвилин. В разі неявки або неможливості виконання МКР з поважних причин на таке заняття допускається відкриття виконання МКР за погодженням з викладачем в інший час асинхронно. Кількість спроб не обмежується, однак обмеження по часу виконання МКР залишається. Кожна модульна контрольна робота включає блок тестових завдань з матеріалу модуля (max 10 балів). Тестові завдання являють собою тести множинного вибору з однією вірною відповіддю. Тести оцінюються за співпадінням з правильною відповіддю.

Додаткові зауваження:

– студент може оскаржити отримані оцінки в порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи : Polytechnic (metinvest.university)) та Положенням про політику та процедури врегулювання конфліктних ситуацій (Академічні політики : Polytechnic (metinvest.university));

– оцінки, отримані за роботу на практичних заняттях, не можуть бути відпрацьовані або покращені, окрім процедури оскарження, оцінки за інші види поточного контролю можуть бути покращені за індивідуальною домовленістю з викладачем;

– викладач не має права знижувати оцінку за індивідуальне завдання або модульну контрольну роботу, якщо вони не були складені вчасно, однак в разі, якщо така робота була оцінена пізніше, ніж момент завершення теоретичного навчання у семестрі, то відповідна оцінка не

враховується у рейтингу здобувачів освіти.

4.3 Форма підсумкового контролю. Порядок визначення підсумкової оцінки

	Варіант вивчення як обов'язкової	Варіант вивчення як вибіркової
Форма підсумковог о контролю	Екзамен, що включає блоки тестових завдань з матеріалу кожного модуля дисципліни.	Залік, тобто підсумкова оцінка вставляється як сума оцінок поточного контролю без проведення додаткових контрольних заходів.
Умови допуску до підсумковог о контролю	Не менше 35 балів; якщо здобувачі освіти в результаті самооцінки академічного прогресу не впевнені, що набравши 35 балів за поточну успішність, складуть іспит на 85 балів і вище, то вони мають підвищити власні результати поточного контролю до прийнятного рівня.	Якщо сума оцінок за поточний контроль за семестр становить менше 60 балів, необхідно відпрацювати відповідні види контролю поточної успішності до звершення теоретичного навчання.
Порядок визначення підсумкової оцінк	Для отримання заліку: – якщо протягом семестру за результатами поточного контролю здобувач освіти набрав менше 60 балів, то під час екзаменаційної сесії йому надається змога отримати/покращити власний результат з усіх видів поточного контролю, крім активності на навчальних заняттях; – в разі, якщо протягом семестру за результатами поточного контролю або в процесі покращення власних результатів здобувач освіти набрав більше 60 балів, йому виставляється фактична сума балів і оцінка «залік», в іншому випадку – «незалік». Для варіанту екзамену. Підсумкова оцінка (ПО) визначається як середнє арифметичне поточної успішності з навчальної дисципліни (О) та оцінки, отриманої під час іспиту (І). В разі, якщо оцінка, отримана на іспиті, менше 60 балів, підсумкова оцінка дорівнює оцінці іспиту: $\begin{cases} ПО = \frac{О + І}{2}, & якщо\ І \geq 60 \\ І, & якщо\ І < 60 \end{cases}$	
Порядок проходженн я екзамену	Екзамен складається в Moodle у визначений розкладом екзаменаційної сесії період; до складу завдань екзамену (100 балів) входять 25 тестових завдань множинного вибору з однією вірною відповіддю (по 4 бали). Екзамен оцінює ступінь володіння теоретичним матеріалом та розуміння технологічних й конструктивних особливостей та програмного й апаратного забезпечення мехатронних систем й робототехнічних комплексів. На складання екзамену надається 3 спроби. Порядок оскарження екзаменаційної оцінки визначений у розділі 10 Положення про організацію освітнього процесу (Нормативні документи : Polytechnic (metinvest.university))	

Відповідність між прийнятими в університеті шкалами оцінки наведена в таблиці.

Бальна шкала	Рівні	Характеристика	Традиційні шкали	
			Іспит	Залік
90-100	A	Студент демонструє видатний рівень досягнення запланованих результатів вивчення навчальної дисципліни, що засвідчують його безумовну готовність до подальшого навчання та/або професійної діяльності за фахом	Відмінно	Залік
82-89	B	Студент виявляє вищий за середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні незначні помилки	Добре	

Бальна шкала	Рівні	Характеристика	Традиційні шкали	
			Іспит	Залік
75-81	C	Студент виявляє середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні деякі значущі помилки		
67-74	D	Студент виявляє задовільний рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях наявні суттєві помилки	Задовільно	
60-66	E	Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати вивчення навчальної дисципліни		
35-59	FX	Низка запланованих результатів навчання не досягнуті. Рівень наявних результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом	Незадовільно	Незалік
0-34	F	Результати навчання відсутні або критично низькі		

4.4 Особливі підходи до визнання результатів навчання

В разі, якщо дисципліна є обов'язковою для здобувача освіти, і він засвоїв повністю або частково відповідні програмні результати навчання під час отримання освіти на попередніх або такому ж рівні, то кредити та оцінка з дисципліни може бути перезарахована в порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи: Polytechnic (metinvest.university)). Консультацію з даного питання можна отримати у викладача, куратора або гаранта освітньої програми, завідувача кафедри, за якою закріплено цю дисципліну;

В разі, якщо здобувач освіти обрав цю дисципліну як дисципліну вільного вибору, не зважаючи на той факт, чи вивчалася вона раніше, оцінка та кредити з цієї дисципліни не перезараховуються;

В разі, якщо здобувач освіти хотів би самостійно вивчити певні курси з проблематики мережі та систем автоматизації (наприклад, Coursera, Udemy або інших платформ, в т.ч. платформ відкритих курсів вітчизняних та/або закордонних університетів), то 1) доцільно звернутися до списку рекомендованих вебресурсів або проконсультуватися з викладачем на предмет релевантності самосійтно знайденого освітнього ресурсу програмі дисципліни; 2) в разі успішності опанування такого курсу, яке підтверджується сертифікатом або іншим способом, такому здобувачу у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи: Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного контролю;

В разі, якщо здобувач освіти реалізував певний вид наукової

роботи (тези, стаття, результативна участь у студентській олімпіаді тощо), то у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи: Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного або навіть підсумкового контролю; консультацію з питань визнання результатів неформальної та інформальної освіти можна отримати в уповноваженої особи від кафедри, яка викладає дисципліну; перелік таких осіб можна знайти за посиланням Студентам: Polytechnic (metinvest.university).

5 РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Базові

1 Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. 2-ге видання, стереотипне. Львів : «Новий Світ- 2000», 2024 . 678 с.
2 Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2022. 135 с.
3 Богуш В. М., Бровко В. Д., Кобус О. С., Козюра В. Д. Технічний захист інформації : навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації. Київ : Видавництво Ліра-К, 2022. 286 с.
4 Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 213 с.
5 Домарєв В. В. Безпека інформаційних технологій. Методи створення систем захисту. Київ : ТзОВ ТІД ДС, 2021. 688 с.
6 Пономаренко В. С., Журавльова І. В. Основи захисту інформації : навчальний посібник. Харків : Вид. ХДЕУ, 2021. 176 с.
7 Євсеєв С. П., Шматко О. В., Ахієзер О. Б., Горбач Т. В. Основи Кібербезпеки: навчальний посібник. Харків - Львів : «Новий Світ-2000», 2025 . 95 с.

Додаткові

1. Subotin O. V. Information security of rental management systems. International scientific conference “MININGMETALTECH 2023 – The mining and metals sector: integration of business, technology and education” : conference proceedings (November 29–30, 2023. Riga, the Republic of Latvia). Riga, Latvia: “Baltija Publishing”, 2023. Vol. 2. Pp. 68 - 71. DOI https://doi.org/10.30525/978-9934-26-361-3-102 .
2. Asaad R. R. Penetration testing: Wireless network attacks method on Kali Linux OS //Academic Journal of Nawroz University. - 2021. - Т. 10. - №. 1. - С. 7-12.
3. Karayat R. et al. Web application penetration testing & patch development using kali linux //2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS). - IEEE, 2022. - Т. 1. - С. 1392-1397.
4. Roshanaei M. Enhancing mobile security through comprehensive penetration testing //Journal of Information Security. - 2024. - Т. 15. - №. 2. - С. 63-86.
5. Kumar B. et al. Kali Linux based Empirical Investigation on Vulnerability Evaluation using Pen-Testing tools //2023 World Conference on Communication & Computing (WCONF). - IEEE, 2023. - С. 1-6.
6. Нікуліна О. М. Аналіз інформаційних технологій для дистанційної ідентифікації динамічних об`єктів / О. М. Нікуліна, В. П. Северин, О.М. Кондратов, Н.Ю. Рекова // Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології. – Харків : НТУ «ХПІ», 2023. – № 1 (9). – С. 110–115. https://repository.kpi.kharkov.ua/items/cc2d6cd1-eed8-46b6-a99b-725a8ca30a13
7. Кондратов О. М., Нікуліна О. М. Ідентифікація параметрів динамічних об’єктів з використанням трансформера з оптичним потоком та ансамблевих методів / О. М. Нікуліна, О.М. Кондратов // Вісник НТУ «ХПІ». Серія: Системний аналіз,

управління та інформаційні технології. – Харків : НТУ «ХПІ», 2025. – № 1 (13). – С. 106–112. http://samit.khpi.edu.ua/article/view/335107/324017

Web-ресурси

1. Інформаційні технології. Аналітичні матеріали : веб-сайт. URL: http://it.ridne.net (дата звернення: 20.08.2024).
2. Networks, AI ets : веб-сайт. URL: https://core.ac.uk/works/43884595 (дата звернення: 20.08.2025).
3. Міністерство освіти і науки України : веб-сайт. URL: https://mon.gov.ua/ (дата звернення: 20.08.2025).
4. Національна бібліотека України ім. Вернадського : веб-сайт. URL: www.nbuv.gov.ua (дата звернення: 20.08.2025).
5. Національна бібліотека України імені Ярослава Мудрого : веб-сайт. URL: https://nlu.org.ua/ (дата звернення: 20.08.2025).
6. Kortext : веб-сайт. URL: https://kortext.com/ (дата звернення: 20.08.2025).
7. Research4life : веб-сайт. URL: https://portal.research4life.org/ (дата звернення: 20.08.2025).
8. Інституційний репозитарій ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА» : веб-сайт. URL: https://dspace.mipolytech.education/home (дата звернення: 20.08.2025).
9. Центральна державна науково-технічна бібліотека гірничометалургійного комплексу України : веб-сайт. URL: http://cgntb.dp.ua/ (дата звернення: 20.08.2025).
10. Metasploit Framework: Penetration Testing with Metasploit : веб-курс. URL: https://ua.udemy.com/course/metasploit-framework-penetration-testing-with-metasploit/ (дата звернення: 20.08.2025).
11. https://www.kali.org/
12. Introduction to Cybersecurity. URL: https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US.

6 АКАДЕМІЧНІ ПОЛІТИКИ

Як член спільноти Технічного університету «МЕТІНВЕСТ ПОЛІТЕХНІКА» Ви маєте дотримуватися певних стандартів та академічної політики:

- ***Академічна недоброчесність*** вигляді академічного плагіату; фабрикації; фальсифікації; списування обману; хабарництва; необ'єктивного оцінювання; надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання – прямо заборонено (докладніше про це – у Положенні про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ТОВ ТЕХНІЧНОГО УНІВЕРСИТЕТУ «МЕТІНВЕСТ ПОЛІТЕХНІКА»); і в разі виявлення – ***відповідний захід контролю (контрольну точку) буде оцінено в 0 балів за з наступним повідомленням декану факультету та голові комісії з академічної доброчесності Університету***.
- В разі випадку надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання студент може оскаржити процедури оцінювання за процедурами, передбаченими Положенням про організацію освітнього процесу (розділ 10).
- Матеріали в рамках курсу, захищені авторським правом, можуть бути використані лише тільки здобувачами освіти, яким призначено даний курс і для цілей, пов'язаних з цим курсом і не можуть поширюватися.
- Спілкування з однокурсниками та викладачем має бути професійним та ввічливим.
- Очікується, що Ви перевірятимете всі Ваші письмові повідомлення, включаючи поштові повідомлення та повідомлення у MS Teams на коректність змісту та мови.
- Використання ШІ не заборонене, разом з тим, воно має здійснюватися відповідально і з урахуванням «живих» політик щодо використання ШІ в Університеті: студент відповідає за повноту, вірогідність інформації, яка була згенерована/знайдена з використанням великих мовних моделей, здатний ідентифікувати у відповіді, яка частина інформації отримана з використанням технологій

ШІ, а що є його власним здобутком/позицією.

– Університет прагне підтримувати середовище, вільне від дискримінації або дискримінаційних домагань, спрямованих на будь-яку людину або групу в межах своєї спільноти - здобувачів освіти, співробітників або відвідувачів.

Докладніше про академічні політики стосовно етичності поведінки, академічної доброчесності та протидію булінгу можна дізнатися за посиланням: Академічні політики - Polytechnic (metinvest.university)