ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ОПИС КУРСУ

Основи кібербезпеки та захисту інформації (ОКЗІ) – 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, аналіз типових загроз і вразливостей інформаційних систем, застосування інструментів тестування на проникнення в навчальному середовищі, розробку та впровадження заходів захисту інформації в корпоративних і розподілених системах.

Особливістю курсу є акцент на: 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. А також підхід із використанням віртуальної лабораторії на базі Kali Linux, дослідження вразливих систем (Metasploitable), аналізу атак типу Brute Force, налаштування безпечного віддаленого доступу (SSH), а також вивчення базових принципів принципів забезпечення конфіденційності, цілісності та доступності даних через сегментацію мереж, криптографічний захист каналів зв'язку та впровадження систем моніторингу й оперативного реагування на кіберінциденти. Дослідженні методів захисту.

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.

Освітній рівень	Бакалавр
Кількість кредитів	4,5
Назва кафедри, яка пропонує дисципліну	Цифрових технологій та проєктно-аналітичних рішень

ШМАТКО Олександр
Oleksandr.Shmatko@mipolytech.education
кандидат технічних наук, доцент, фахівець в сфері інтелектуального аналізу даних, Data Mining, застосування методів та моделей інтелектуального аналізу даних в кібербезпеці

КОНДРАТОВ Олексій
Oleksii.Kondratov@mipolytech.education
старший викладач, наукові інтереси: Artificial Intelligence, Software Development, Operating Systems, Web-Technologies, Software Systems, Devops, кібербезпека, моделювання, алгоритми

ВИМОГИ

- базові знання зі спеціальності: схемотехніка та архітектура комп'ютерів, системний аналіз, комп'ютерні мережі, проєктування інформаційних систем та програмного забезпечення, операційних систем;
- підготовка з інформатики: використання Microsoft Word, Excel та Visio, базові знання з алгоритмізації та програмування;- наявність корпоративного облікового запису @mipolytech.education, Microsoft Teams;
- 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.

ТЕМАТИКА

Загальні поняття захисту інформації; Закони України про захист інформації; цілі інформаційної безпеки; управління інформацією про безпеку та події (SIEM); визначення, що використовуються в сфері інформаційної безпеки; зони безпеки мережі. Концепції забезпечення інформаційної безпеки: принципи забезпечення безпеки в комп'ютерних системах; криптографічний захист інформації. Захист віддаленого доступу: безпечне управління, захист площини управління (MPP); концепції організації автентифікації, авторизації та аудиту(AAA). Операційні системи та безпека. Linux як платформа для дослідження безпеки. Віртуалізація та побудова навчальних лабораторій з кібербезпеки. Kali Linux: архітектура, інструменти, етичні аспекти використання. Вразливості інформаційних систем. Metasploitable як навчальне середовище. Дослідження бекдорів та експлуатація вразливостей (у навчальних цілях). Захист віддаленого доступу. SSH, принципи безпечної конфігурації. Brute Force атаки: методи реалізації та способи захисту. Система комлексного захисту інформації.

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 та програмної обробки їх результатів – з іншого.

Відвідування лекційних занять є бажаним, однак не обов'язковим; від студентів очікується ознайомлення з матеріалом перед лекцією, що дозволить побудувати лекційне заняття у вигляді сполучення пояснень викладача та обговорення проблемних питань, які виникли при підготовці до лекції.

Практичні заняття передбачають розбір теоретичних та практичних питань з вивчення способів та засобів проєктування, розробки та моделювання корпоративних обчислювальних мереж, а також вивчення критеріїв, методів та засобів забезпечення інформаційної безпеки. Практичні заняття орієнтовані на виконання лабораторних робіт із використанням Kali Linux та вразливих тестових систем.

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.

ПІДХОДИ ДО ОЦІНЮВАННЯ

Розподіл балів за контрольними точками та графік їх виконання

Дисципліна є обов'язковим 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

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

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 (max 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 та/або групи, вміння вести дискусію та бути критичним та самокритичним (5 бали).
Виконання та захист індивідуальних завдань за модулем 1, 2 та 3: М1. «Розгортання лабороторії та аналіз безпеки віртуальної лабораторії Kali Linux і Metasploitable»; М2. «Захист віддаленого доступу. Конфігурація та захист SSH у Kali Linux та дослідження інструментів Brute Force Attack та методів захисту»; М3. «Дослідження методів захисту»	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 та задач з матеріалу модуля (max 20 балів). Тестові завдання являють собою тести множинного вибору з однією вірною відповіддю. Задачі передбачають обґрунтування порядку розв'язання проблем, виконання розрахунків. 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.

Форма підсумкового контролю. Порядок визначення підсумкової оцінки

	Варіант вивчення як обов'язкової	Варіант вивчення як вибіркової
Форма підсумкового 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 підсумкового 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 проходження 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	
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		

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 (дисципліни «Політична економія», «Мікроекономіка», «Макроекономіка», «Основи економічної теорії»), 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 економічної теорії (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; перелік таких осіб можна знайти за посиланням Студентам : Polytechnic (metinvest.university).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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.
8 Introduction to Cybersecurity. URL: https://www.netacad.com/courses/ introduction-to-cybersecurity?courseLang=en-US.

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)