МЕЛІТОПОЛЬСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО

ФАКУЛЬТЕТ ІНФОРМАТИКИ, МАТЕМАТИКИ ТА ЕКОНОМІКИ

Кафедра інформатики і кібернетики

Назва курсу *Нормативний/вибірковий*	**Захист інформації** *Вибіркова*
Ступінь освіти **Освітня програма**	**Магістр** Середня освіта. Інформатика Професійна освіта. Комп'ютерні технології Цифровий дизайн Комп'ютерні науки
Рік викладання / Семестр	*2024-2025 / парний семестр*
Сторінка курсу в ЦОДТ МДПУ ім. Б.Хмельницького	https://dfn.mdpu.org.ua/course/view.php?id=404
Консультації	Очні консультації: згідно графіку роботи кафедри інформатики і кібернетики. Онлайн-консультації: через систему ЦОДТ МДПУ ім. Б. Хмельницького.

1. АНОТАЦІЯ

Навчальна дисципліна «Захист інформації» зорієнтована на набуття початкових знань з кібербезпеки. Під час її вивчення ви дізнаєтесь про основи апаратного та програмного захисту даних в інформаційних системах, зрозумієте алгоритми, що використовуються в таких системах.

2. МЕТА КУРСУ

Метою дисципліни є набуття студентами знань з теоретичних і практичних аспектів захисту інформації; формування практичних навичок у сфері забезпечення захисту даних в інформаційних системах різних типів, здатності до попередження можливих небезпек і ризиків втрати інформації або несанкціонованого доступу до неї.

3. ОБСЯГ КУРСУ

Вид заняття	**Загальна кількість**	**Лекції**	**Практичні/ лабораторні заняття**	**Самостійна робота**
Кількість годин	**120 годин**	**40 годин**	**18 годин**	**62 годин**

4. ПОЛІТИКА КУРСУ

Політика навчання через дослідження:

- Курс є складовою освітньо-професійної програми, тому усі його складові розглядаються у контексті відповідності наукових інтересів бакалаврів.

Політика академічної поведінки та етики:

- Не пропускати та не запізнюватися на заняття за розкладом;
- Вчасно виконувати завдання семінарів та питань самостійної роботи;
- Вчасно та самостійно виконувати контрольно-модульні завдання.
- Дотримуватись Кодексу академічної доброчесності, прийнятого у МДПУ імені Богдана Хмельницького https://mdpu.org.ua/wp-content/uploads/2020/11/Kodeks-akadem-dobrochesnosti_2020.pdf та Положення про Академічну доброчесність https://mdpu.org.ua/wp-content/uploads/2020/11/akademichna-dobrochesnist_2020.pdf. Здобувачі освіти мають самостійно виконувати навчальні завдання, завдання поточного та періодичного контролю, самостійні завдання, посилатися на джерела інформації у разі запозичень ідей, тверджень, відомостей; дотримуватись норм законодавства про авторське право.

Політика щодо дедлайнів та перескладання: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Поточний контроль: усне опитування в ході лекцій та практичних занять, перевірка завдань (у тому числі самостійної роботи), оцінювання правильності вирішення тестових та практичних завдань на семінарських заняттях.

5. СТРУКТУРА КУРСУ

5.1. СТРУКТУРА ВСЬОГО КУРСУ

№	Тема	Форма діяльності (заняття, кіл-ть годин)	Літер атура	Завдання	Вага оцінки	Термін виконання
Блок 1.						
1	Проблема захисту інформації	Лекція (2)	1 - 8	Відповіді на контрольні питання до лекції	-	перший періодичний контроль
2	Методи та рівні захисту інформації	Лекція (2)	1 - 8	Відповіді на контрольні питання до лекції	-	
3	Паролі і механізми контролю за доступом	Лекція (2) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
4	Криптографія	Лекція (4)	1 - 8	Відповіді на контрольні	-	

				питання до лекції		
5	Алгоритми з секретним ключем	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
6	Алгоритми с відкритим ключем	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	-	
Блок 2.						
7	Потокові алгоритми	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	другий періодичний контроль
8	Алгоритми хешування	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
9	Криптоаналіз	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
10	Цифрові підписи	Лекція (2) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
11	Мережеві протоколи захисту	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	
12	Захист сайтів	Лекція (4) Лабораторна робота (2)	1 - 8	Виконання завдань лабораторної роботи	5	

5.2. СТРУКТУРА КУРСУ (ЛЕКЦІЙНИЙ БЛОК)

№ з/п	Назва теми лекції та питання, що вивчаються
1.	**Проблема захисту інформації** Постановка проблеми. Класифікація типів та причин ушкодження інформації. Класифікація способів перевірки прав користувачів. Класифікація способів захисту. Класифікація способів зламу.
2.	**Методи та рівні захисту інформації** Програмні методи. Апаратні методи. Адміністративні методи. Методи захисту локального комп'ютера. Методи захисту в локальній мережі. Методи захисту в глобальних мережах.
3.	**Паролі і механізми контролю за доступом** Парольний захист і випадки його використання. Контроль та моніторинг доступу. Методи перевірки паролю. Методи підбору паролю.

№ з/п	Назва теми лекції та питання, що вивчаються
4.	**Шифрування** Симетричні криптосистеми. Криптосистеми з відкритим ключем. Системи керування ключами. Сертифікатні та сертифікаційні центри.
5.	**Алгоритми з секретним ключем** Алгоритми та системи шифрування з секретним ключем DES, RC2, RC5, IDEA, SAFER, REAL, Blowfish.
6.	**Алгоритми с відкритим ключем** Алгоритм RSA, його криптостійкість та швидкість роботи. Алгоритм Ель-Гамаля, його криптостійкість.
7.	**Потокові алгоритми** Регістри зсуву зі зворотним зв'язком. Алгоритми A5, RC4, SEAL.
8.	**Алгоритми хешування** Поняття про хешувальні алгоритми, їх призначення, вимоги до них. Колізійно-стійкі функції хешування Whirpool, SHA-256, SHA-384, SHA-512. Алгоритми сімейства MD. Алгоритми SHA-1, SHA-2.
9.	**Цифровий підпис** Поняття про цифровий підпис (на прикладі RSA), вимоги до нього. Основні алгоритми електронного цифрового підпису. DSA. Стандарти ЕЦП. Український алгоритм ЕЦП ДСТУ 4145.
10.	**Мережеві протоколи захисту** Протокол IPSec. Протокол SSL. Протокол TLS.
11.	**Захист сайтів** Класифікація методів зламу сайтів за об'єктами атаки. Використання звичок користувачів для зламу сайтів. Використання необізнаності користувачів для зламу сайтів. Атака на хостинг. Атака на ядро сайту. Скрипт-ін'єкції клієнтські та серверні. SQL-ін'єкції. Загальні підходи до захисту сайтів. Методи протидії підбору паролів.

5.3. СТРУКТУРА КУРСУ (ПРАКТИЧНЕ ЗАНЯТТЯ)

№ з/п	Назва теми та зміст роботи
1.	**Тема**: Методи та рівні захисту інформації **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
2.	**Тема**: Паролі і механізми контролю за доступом **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
3.	**Тема**: Криптографія. **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
4.	**Тема**: Алгоритми з секретним ключем **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
5.	**Тема**: Алгоритми с відкритим ключем **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань

№ з/п	Назва теми та зміст роботи
6.	**Тема**: Потокові алгоритми **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
7.	**Тема**: Алгоритми хешування **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
8.	**Тема**: Цифрові підписи **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
9.	**Тема**: Мережеві протоколи захисту. **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань
10.	**Тема**: Захист сайтів **Зміст** 1. Актуалізація теоретичних знань з теми 2. Виконання практичних завдань

5.4 СТРУКТУРА КУРСУ (ТЕМИ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ)

№ з/п	Теми і перелік питань, що винесені на самостійне вивчення
1.	**Тема 1.** Проблема захисту інформації Поняття про інформацію з обмеженим доступом. Основні задачі, які повинні вирішуватися системою комп'ютерної безпеки.
2.	**Тема 2.** Методи та рівні захисту інформації Структура політики безпеки та її основні частини. Життєвий цикл розробки систем безпеки.
3.	**Тема 3.** Паролі і механізми контролю за доступом TCSEC ("Оранжева книга") – перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria ("Загальні критерії") – європейський стандарт у галузі оцінки захищеності комп'ютерних систем. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу".
4.	**Тема 4.** Криптографія Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах". Класифікація сучасних криптосистем та основні вимоги до них.
5.	**Тема 5.** Алгоритми з секретним ключем Огляд алгоритмів українського конкурсу на сертифікований симетричний криптоалгоритм: RSB-32, "Мухомор", "Калина", "Лабіринт".
6.	**Тема 6.** Алгоритми с відкритим ключем Наукова основа. Криптографія з кількома відкритими ключами.
7.	**Тема 7.** Потокові алгоритми Проектування потокових шифрів. Атаки на потокові шифри.
8.	**Тема 8.** Алгоритми хешування Алгоритм хешування SHA-3.
9.	**Тема 9.** Криптоаналіз Історія криптоаналізу. Методи криптоаналізу за Б. Шнаєром. Класифікація атак на симетричні криптоалгоритми. Класифікація атак на асиметричні криптоалгоритми.

№ з/п	Теми і перелік питань, що винесені на самостійне вивчення
	Диференціальний криптоаналіз. Лінійний криптоаналіз.
10.	**Тема 10.** Цифрові підписи Юридична значимість ЕЦП. Політична роль ЕЦП. Обмеження використання національного ЕЦП.
11.	**Тема 11.** Мережеві протоколи захисту Основні принципи захисту інформації при підключені до мережі Інтернет. Захист інформації за допомогою міжмережних екранів.
12.	**Тема 12.** Захист сайтів Проблема зламу сайтів. Атака на контент сайту. Протидія SQL-ін'єкціям.

6. ФОРМИ КОНТРОЛЮ І МЕТОДИ НАВЧАННЯ

Оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до «Положення про бально-накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти у МДПУ імені Богдана Хмельницького».

Форми контролю: поточний та періодичний контроль, підсумковий семестровий контроль (залік).

Методи навчання. Студентсько-центроване навчання. Професійно-орієнтоване навчання, індивідуально-творчий підхід. Очний (*offline*) у вигляді лекційних та семінарських занять. Змішаний (*blended*) через систему Центру освітніх дистанційних технологій МДПУ імені Б.Хмельницького, Zoom, Інтернет. Усі складові курсу розглядаються у контексті відповідності наукових інтересів бакалаврів.

Словесні методи (розповідь, лекція); наочні методи (ілюстрування, демонстрування); лабораторні роботи; методи стимулювання та мотивації навчально-пізнавальної діяльності; інтерактивні методи (дослідні методи (проєкт), мозковий штурм), самостійна робота студентів.

7. СИСТЕМА ОЦІНЮВАННЯ ТА ВИМОГИ

Практичні заняття	***«5»*** *– студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому нормативну, обов'язкову та додаткову літературу. Правильно вирішив усі розрахункові / тестові завдання. Здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно-наслідкові зв'язки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями.* ***«4»*** *– студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому нормативну та обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість розрахункових / тестових завдань. Студент здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно-наслідкові зв'язки, у яких можуть бути окремі несуттєві помилки, формувати висновки і узагальнення, вільно оперувати фактами та відомостями.* ***«3»*** *– студент в цілому володіє навчальним матеріалом, викладає*

	його основний зміст під час усних виступів та письмових розрахунків, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину розрахункових / тестових завдань. Має ускладнення під час виділення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв'язків і формулювання висновків. ***«2»** – студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових розрахунків, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив окремі розрахункові / тестові завдання. Безсистемно відділяє випадкові ознаки вивченого; не вміє зробити найпростіші операції аналізу і синтезу; робити узагальнення, висновки.* ***«1»** – студент виконав менше половини завдання практичної роботи або не виконав зовсім; під час усних відповідей не розкриває зміст теоретичних питань та практичних завдань. Не відповідає на елементарні питання.*
Періодичний контроль знань і вмінь студентів	***60 балів*** *За кожний ПМК максимум 30 балів:* *30 тестових питань, 1 питання оцінюється в 1 бал (за принципом вірна відповідь – 1 бал, не вірна – 0).*
Умови допуску до підсумкового контролю	*Студент зобов'язаний відпрацювати всі пропущені лабораторні заняття протягом двох тижнів. Невідпрацьовані заняття (невиконання навчального плану) є підставою для недопущення студента до підсумкового контролю.*
Підсумковий контроль	*Підсумковим контролем вивчення навчальної дисципліни є недиференційований залік. Набраних протягом семестру 60 і більше балів достатньо для його зарахування.*

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**
		для заліку
90 – 100	**A**	зараховано
82-89	**B**	
74-81	**C**	
64-73	**D**	
60-63	**E**	
35-59	**FX**	не зараховано з можливістю повторного складання
0-34	**F**	не зараховано з обов'язковим повторним вивченням дисципліни

8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНФОРМАЦІЙНІ РЕСУРСИ

Основна

1. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.
3. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. Київ, 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. Київ: ФОП Москаленко О. М., 2017. 72 с.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: «Новий Світ-2000», 2020 . 678 с.
5. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах». Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
6. Abolhassan F. (Ed.). Cyber Security. Simply. Make it Happen. Leveraging Digitization Through IT Security. Cham, Switzerland: Springer International Publishing AG, 2017. 136 p.
7. Dykstra J. Essential Cybersecurity Science. Build, Test, and Evaluate Secure Systems. Sebastopol, CA: O'Reilly Media, Inc., 2016. 190 p.
8. Pande J. Introduction to Cyber Security. Haldwani: Uttarakhand Open University, 2017. 152 p.

Допоміжна

1. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика*. Житомир: Вид-во ЖДУ, 2013. 136 с.
2. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. К., 2013. 435 с.
3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. Киів: BHV, 2009.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації : навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.
5. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: ЮНИОР, 2003.
6. Vacca J.R. (Ed.). Cyber security and IT infrastructure protection. Waltham, MA: Elsevier, 2014. 381 p.

Інформаційні ресурси в Інтернеті

1. Журнал «Захист інформації». URL: http://jrnl.nau.edu.ua/index.php/ZI/index
2. https://www.commoncriteriaportal.org
3. https://wiki.tntu.edu.ua/Класифікація_криптоалгоритмів