Міжнародний гуманітарний університет

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук

Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Галузь знань 01 Освіта
Спеціальність 014.09 Середня освіта (Інформатика)
Назва освітньої програми Інформатика та програмування
Рівень вищої освіти перший (бакалаврський)

Розробники і викладачі	Контактний тел.	E-mail
зав. кафедри комп'ютерної інженерії та інноваційних технологій к.т.н., доцент **Йона Лариса Григорівна**	+380 67 746 37 77	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Дисципліна «Безпека програм та даних» є обов'язковою складовою професійної підготовки бакалаврів за спеціальністю 014 «Середня освіта» та спрямована на формування у майбутніх учителів системного розуміння принципів, методів і засобів забезпечення безпеки програмного забезпечення та даних в освітньому інформаційному середовищі.

Курс охоплює фундаментальні та прикладні аспекти захисту програмного середовища, зокрема архітектурні принципи безпеки, моделі контролю доступу, налаштування захищеного оточення операційних систем, захист від поширених загроз, мережеву фільтрацію та управління вразливостями. Значна увага приділяється практичному застосуванню криптографічних механізмів, управлінню паролями та ключовою інформацією, захищеним протоколам передачі даних, організації безпечних з'єднань, а також захисту персональних даних у хмарних середовищах, що використовуються в освітньому процесі.

Вивчення дисципліни забезпечує формування у здобувачів здатності навчати учнів основам кібергігієни, проєктувати безпечне інформаційне середовище закладу освіти, здійснювати моніторинг стану захищеності шкільних комп'ютерних мереж, виявляти типові вразливості

та реагувати на інциденти інформаційної безпеки в межах компетентності вчителя інформатики. Практична складова курсу реалізується через виконання лабораторних робіт у віртуалізованому середовищі з використанням сучасних інструментів захисту, доступних для навчальних цілей.

МЕТА ДИСЦИПЛІНИ. Метою дисципліни є формування у майбутніх педагогів цілісного уявлення про безпеку програмного забезпечення та даних і розвиток практичних навичок застосування технічних, програмних і криптографічних засобів захисту для потреб освіти. Зміст дисципліни узгоджено з освітньо-професійною програмою підготовки фахівців за спеціальністю 014 «Середня освіта» та шкільною програмою з інформатики. Він забезпечує необхідну теоретичну й практичну базу для кваліфікованого викладання розділів з інформаційної безпеки, а також для формування у здобувачів навичок безпечної поведінки в цифровому середовищі.

ПРЕРЕКВІЗИТИ. Передумовами є знання з програмування "Комп'ютерна схемотехніка та архітектура комп'ютерів", "Операційні системи", "Організація баз даних та знань", "Програмування мікроконтролерів та робототехніка в закладах освіти".

ПОСТРЕКВІЗИТИ. Знання та навички із захисту програм та даних є необхідними при проходженні педагогічної практики.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни формуються наступні компетентності та результати навчання із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі у галузі освіти, інформатики та інформаційних технологій, що передбачає застосування певних теорій і методів педагогічних та комп'ютерних наук і характеризується комплексністю та невизначеністю умов.

Загальні компетентності

ЗК9. Здатність виявляти ініціативу та підприємливість; здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК10. Здатність використовувати інформаційно-комунікаційні технології з дотриманням етично-правових норм в умовах євроінтеграційних процесів.

Фахові компетентності (ФК)

ФК7. Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійній діяльності.

ФК8. Здатність використовувати цифрові технології в освітньому процесі, створювати та використовувати цифрові освітні ресурси.

ФК11. Здатність використовувати навчально-методичний інструментарій, обладнання навчального й загального призначення для кабінетів інформатики, мультимедійне обладнання.

ФК18. Здатність налагоджувати, конфігурувати, обслуговувати та діагностувати комп'ютерні, мережеві та роботизовані системи, периферійні пристрої; встановлювати, оновлювати та адмініструвати програмне забезпечення та забезпечувати його стабільну і безпечну експлуатацію в освітньому середовищі.

Фахові програмні результати навчання (РН)

РН11. Орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, перевіряти її достовірність, оперувати нею у професійній діяльності.

РН12. Дотримуватися академічної доброчесності, вимог щодо охорони авторських прав під час використання та поширення електронних (цифрових) освітніх ресурсів.

Предметні програмні результати навчання (ПРН)

ПРН3. Налагоджувати, конфігурувати, обслуговувати та діагностувати комп'ютерну техніку, комп'ютерні мережі та роботизовані системи; встановлювати, оновлювати та адмініструвати програмне забезпечення, забезпечувати його стабільне та безпечне функціонування.

ПРН6. Застосовувати засоби й методи захисту інформації та безпеки в мережі Інтернет.

Заплановані результати навчання за навчальною дисципліною

Знання:

– фундаментальні принципи, моделі та стандарти забезпечення безпеки програмного забезпечення та даних в освітньому інформаційному середовищі;

– архітектурні підходи до побудови захищених систем, моделі контролю доступу (DAC, MAC, RBAC) та механізми автентифікації;

– основи криптографії: симетричні та асиметричні алгоритми, хеш-функції, цифрові підписи та протоколи захищеної передачі даних;

– методи виявлення, аналізу та мінімізації вразливостей програмних систем, принципи захисту від автоматизованих атак;

– особливості захисту персональних даних, організації безпечних з'єднань та роботи з хмарними сервісами в освітньому процесі;

– нормативно-правові засади та стандарти інформаційної безпеки, вимоги до дотримання академічної доброчесності та авторських прав.

Уміння:

– аналізувати загрози безпеці програм та даних і обґрунтовано обирати відповідні засоби захисту для освітніх потреб;

– налаштовувати параметри безпеки операційних систем, фаєрволів та мережевого обладнання в комп'ютерних класах;

– застосовувати криптографічні інструменти для захисту файлів, повідомлень та резервних копій навчальних матеріалів;

– виявляти типові вразливості програмного забезпечення та вживати заходів щодо їх усунення в межах компетентності вчителя;

– організовувати безпечне цифрове середовище для дистанційного та змішаного навчання з дотриманням вимог захисту даних;

– адаптувати технічні знання з кібербезпеки для методично обґрунтованого викладання у закладах середньої освіти.

Навички:

– встановлювати, конфігурувати та оновлювати програмне забезпечення з урахуванням вимог інформаційної безпеки в освітньому середовищі;

– використовувати засоби моніторингу, журналювання та аудиту для оцінки стану захищеності шкільних інформаційних систем;

– застосовувати віртуалізовані середовища та сучасні інструменти захисту для проведення навчальних лабораторних робіт з кібербезпеки;

– реагувати на інциденти інформаційної безпеки, здійснювати збір та первинний аналіз цифрових доказів у межах педагогічної діяльності;

– формувати у здобувачів освіти навички цифрової гігієни, безпечної поведінки в мережі та критичного оцінювання інформації;

– проєктувати та впроваджувати комплексні заходи захисту програм і даних з урахуванням вікових особливостей учнів та вимог освітніх стандартів.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)				**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Лабораторні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
5	150	42/12		26/8	82/130	3/3	6/6	**Обов'язкова**

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	**Кількість годин**									
	денна форма					**Заочна форма**				
	усього	**у тому числі**				**усього**	**у тому числі**			
		лекц.	**лаб.**	**прак.**	**сам. роб.**		**лекц.**	**лаб.**	**прак.**	**сам. роб.**
Змістовий модуль 1. Безпека програмного середовища та операційних систем **Тема 1.** Архітектурні основи безпеки програм та даних. Академічна доброчесність та етична відповідальність у сфері безпеки програм і даних.	8	2			6	10	2			8
Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища	12	4		2	6	12			2	10
Тема 3. Моделі контролю доступу та безпека облікових записів	12	4		2	6	12	2			10
Тема 4. Аудит безпеки та оцінка стану захищеності операційних систем	10	2		2	6	10			2	8
Тема 5. Захист від атак грубої сили та автоматизованих вторгнень	10	4		2	4	12				12
Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах	10	2		2	6	10	2			8
Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки	10	2		2	6	8				8
Змістовий модуль 2. Захист даних та безпечна комунікація **Тема 8.** Криптографічні механізми захисту даних у програмних системах	10	2		2	6	12				12
Тема 9. Управління криптографічними ключами та довірчою інфраструктурою	10	2		2	6	12	2			10
Тема 10. Захищені протоколи передачі даних та їх реалізація	12	4		2	6	10			2	8
Тема 11. Віртуальні приватні мережі та організація захищених тунелів	12	4		2	6	10	2			8
Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах	12	4		2	6	12	2		2	8

Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази	10	2		2	6	12				12
Тема 14. Стандарти та комплексний підхід до захисту програм і даних	12	4		2	6	8				8
Усього годин	**150**	**42**		**26**	**82**	**150**	**12**		**8**	**130**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «**Безпека програм та даних**» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Змістовий модуль 1. Безпека програмного середовища та операційних систем** **Тема 1. Архітектурні основи безпеки програм та даних** Поняття безпеки програмного забезпечення та даних. Модель CIA (конфіденційність, цілісність, доступність) як основа побудови систем захисту. Принципи безпечного проєктування: defense in depth, принцип найменших привілеїв, мінімальна поверхня атаки. Академічна доброчесність та етична відповідальність у сфері безпеки програм і даних. Дотримання авторських прав при використанні програмного коду та цифрових ресурсів. Прийняття рішень у сфері IT-безпеки з урахуванням принципів доброчесності та запобігання недоброчесним практикам.	6	8
2	**Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища** Принципи ізоляції процесів і ресурсів в операційних системах. Віртуалізація як інструмент забезпечення безпеки та моделювання атак і захисних механізмів. Типи віртуалізації та їх вплив на рівень захищеності. Контейнери як легковаговий механізм ізоляції. Використання віртуальних середовищ для аналізу вразливостей і тестування	6	10

	політик безпеки.		
3	**Тема 3. Моделі контролю доступу та безпека облікових записів** Моделі контролю доступу: дискреційна (DAC), обов'язкова (MAC), рольова (RBAC). Ідентифікація, автентифікація та авторизація користувачів. Управління обліковими записами користувачів і служб. Політики паролів, багатофакторна автентифікація. Принцип найменших привілеїв у багатокористувацьких операційних системах.	6	10
4	**Тема 4. Аудит безпеки та оцінка стану захищеності операційних систем** Поняття аудиту безпеки та його місце в життєвому циклі системи захисту. Етапи проведення аудиту: збір інформації, аналіз, оцінка ризиків, формування рекомендацій. Стандарти та методики аудиту (CIS Benchmarks, NIST SP 800). Автоматизовані інструменти аудиту безпеки. Інтерпретація результатів перевірки та формування заходів з підвищення рівня захищеності.	6	8
5	**Тема 5. Захист від атак грубої сили та автоматизованих вторгнень** Характеристика атак типу brute force, dictionary attack, credential stuffing. Джерела даних для виявлення атак: журнали автентифікації, системні логи, мережеві події. Принципи роботи систем виявлення та запобігання вторгненням (IDS/IPS). Реалізація механізмів автоматичного блокування зловмисних дій. Налаштування параметрів реагування та оцінка ефективності захисту.	4	12
6	**Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах** Поняття мережевого фаєрволу та його роль у захисті програмного середовища. Архітектура фільтрації трафіку. Типи фільтрації: за адресами, портами, протоколами, станом з'єднання. Таблиці та ланцюги правил. Трансляція мережевих адрес (NAT) як елемент безпеки. Логування мережевих подій і підготовка до аналізу інцидентів.	6	8
7	**Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки** Роль оновлень у запобіганні експлуатації відомих вразливостей. Поняття CVE та CVSS. Процес управління вразливостями. Перевірка цілісності програмних пакетів. Автоматизація оновлення безпеки. Управління конфігураціями як складова підтримки безпечного стану системи.	6	8
	Змістовий модуль 2. Захист даних та безпечна комунікація **Тема 8. Криптографічні механізми захисту даних у програмних системах** Роль криптографії у забезпеченні конфіденційності, цілісності та автентичності даних. Симетричні та асиметричні алгоритми шифрування. Криптографічні хеш-функції та цифрові підписи. Практичне застосування криптографії для захисту файлів, повідомлень і резервних копій. Типові помилки при самостійному впровадженні криптографічних механізмів.	6	12
	Тема 9. Управління криптографічними ключами та довірчою інфраструктурою Життєвий цикл криптографічних ключів: генерація, зберігання, розповсюдження, ротація, відклик та архівація. Ризики компрометації ключової інформації. Апаратні та програмні засоби захисту ключів (HSM, TPM, токени). Основи інфраструктури відкритих ключів (PKI). Нормативні вимоги та стандарти управління ключами.	6	10
	Тема 10. Захищені протоколи передачі даних та їх реалізація Принципи побудови захищених протоколів передачі даних. Протоколи SSH, TLS/SSL, IPsec та їх призначення. Процеси автентифікації, узгодження параметрів безпеки та обміну ключами. Сертифікати X.509 та ланцюги довіри. Типові помилки конфігурації захищених протоколів та їх наслідки.	6	8

	Тема 11. Віртуальні приватні мережі та організація захищених тунелів Поняття віртуальної приватної мережі (VPN) та сфери її застосування. Топології VPN: site-to-site та remote access. Протокол IPsec: компоненти AH, ESP, IKE, режими transport і tunnel. Порівняння IPsec, OpenVPN та WireGuard. Практичні аспекти побудови захищених мережевих тунелів.	6	8
	Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах Особливості зберігання та обробки даних у розподілених системах. Захист даних «at rest» та «in transit». Управління секретами та обліковими даними сервісів. Модель Zero Trust як сучасний підхід до безпеки. Ізоляція ресурсів та мінімізація привілеїв у хмарних і контейнерних середовищах.	6	8
	Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази Роль моніторингу у забезпеченні безпеки програм і даних. Джерела подій безпеки: системні та прикладні журнали, мережеві логи. Основи реагування на інциденти інформаційної безпеки. Збір, збереження та первинний аналіз цифрових доказів. Забезпечення відновлення штатного функціонування систем після інцидентів.	6	12
	Тема 14. Стандарти та комплексний підхід до захисту програм і даних Нормативні та міжнародні стандарти у сфері захисту інформації (ISO/IEC 27001, ДСТУ, вимоги регуляторів). Вимоги до криптографічного захисту. Аудит відповідності політикам безпеки. Інтеграція організаційних, програмних і технічних засобів у комплексну систему захисту програм і даних.	6	8
	Всього	**82**	**130**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, залік, екзамен

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(поточний контроль, підсумковий контроль, загальний результат оцінювання)

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;

[1] Індивідуально-консультативна робота викладача зі здобувачами

- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за пдготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гумані-

тарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України “Про освіту” академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». – Запоріжжя : ЗНУ, 2022. – 72 с.
2. Сенів М. М. Безпека програм та даних : навч. посібник / М. М. Сенів, В. С. Яковина. – Львів : Львівська політехніка, 2015. – 256 с.
3. Дем'яненко В. А. Безпека програм та даних [Електронний ресурс] : навч. посіб. до лаб. практикуму / В. А. Дем'яненко, Ю. А. Кузнецова. — Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. — 95 с.
4. Євсеєв С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навчальний посібник / С. П. Євсеєв, О. В. Мілов, О. Г. Король. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 222 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : Вид-во «Політехніка» КПІ ім. Ігоря Сікорського, 2021. – 213 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. – Х. : ХНЕУ, 2018. – 510 с.
7. Мамченко С. М. Комплексні системи захисту інформації: навч. посіб. / С. М. Мамченко, В. Д. Козюра, В. Д. Бровко. – Київ: Нац. Акад. СБУ, 2018. – 372 с.

Допоміжна

8. Остапов С. Є. Технології захисту інформації / С. Є. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці : Видавничий дім «Родовід», 2014. - 428 с.
9. Захист інформації в автоматизованих системах управління : навч. посібник / уклад.: І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. - 226 с.
10. Літнарович Р. М. Сучасні технології інформаційної безпеки : навч. посібник. – Рівне : МЕГУ, 2011. – 97 с.
11. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. — Харків : Вид-во ХНЕУ, 2010. – 316 с.
12. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2018. – С. 10–14.
13. Дудатьєв А. В. Захист програмного забезпечення. Ч. 1 : навч. посібник / А. В. Дудатьєв, В. А. Каплун, В. П. Семеренко. - Вінниця : ВНТУ, 2005. – 140 с.
14. Мельник І. В. Інформаційні комп'ютерні мережі : навч. посібник для дист. навчання. –К. : Вид-во Універ. «Україна», 2006. – 250 с.
15. Богуш В. М., Давидьков О. А. Теоретичні основи захищених інформаційних технологій. – К. : ДУІКТ, 2010. – 414 с.
16. Довгань О. Д. Методологія захисту інформації: навч.-метод. посіб. / О. Д. Довгань, Г. М. Гулак, А. К. Гринь, С. В. Мельник. – К. : Наук.-вид. центр НА СБ України, 2012. – 184 с.
17. Ленков С. В. Методи і засоби захисту інформації / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; за ред. В. А. Хорошко. – К. : Арий, 2008. – Т. ІІ. Інформаційна безпека. –344 с.
18. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К. : Видавнича група BHV, 2009. — 608 с.
19. Юдін О. К., Корченко О. Г., Конахович В. Г. Захист інформації в мережах передачі даних. – К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 716 с.

Інформаційні ресурси

1. Національна бібліотека України ім. В. І. Вернадського : URL: http://www.nbuv.gov.ua.
2. Он-лайн бібліотека «Лібком» : URL: http://www.lib.com.ua.
3. MIT OpenCourseWare (OCW) : URL: https://ocw.mit.edu/.
4. Dive into Systems : URL: https://diveintosystems.org/.
5. Open Textbook Library : URL: https://open.umn.edu/opentextbooks.
6. Directory of Open Access Books (DOAB) : URL: https://www.doabooks.org/.
7. Internet Engineering Task Force (IETF) : URL: https://www.ietf.org/.
8. RFC Editor : URL: https://www.rfc-editor.org/.

9. National Institute of Standards and Technology (NIST) – Computer Security Resource Center : URL: https://csrc.nist.gov/.
10. OWASP (Open Web Application Security Project) : URL: https://owasp.org/.
11. IEEE Standards Association : URL: https://standards.ieee.org/.
12. Wireshark Documentation : URL: https://www.wireshark.org/docs/.
13. SANS Institute Reading Room : URL: https://www.sans.org/white-papers/.
14. ENISA (European Union Agency for Cybersecurity) : URL: https://www.enisa.europa.eu/.