Силабус курсу:

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Ступінь вищої освіти:	бакалавр
Спеціальність:	126 «Інформаційні системи та технології»
Рік підготовки:	2
Семестр викладання:	весняний
Кількість кредитів ЄКТС:	5
Мова(-и) викладання:	українська
Вид семестрового контролю	екзамен

Автор курсу та лектор:

к.т.н., доц. Митрохін Сергій Олександрович

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

доцент кафедри програмування та математики

посада

mytrokhin@snu.edu.ua	+38-095-208-38-36	WhatsApp	301 НК, за розкладом
електронна адреса	телефон	месенджер	консультації

Викладач лабораторних занять:*

к.т.н., доц. Митрохін Сергій Олександрович

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

доцент кафедри програмування та математики

посада

mytrokhin@snu.edu.ua	+38-095-208-38-36	WhatsApp	301 НК, за розкладом
електронна адреса	телефон	месенджер	консультації

Викладач практичних занять:*

вчений ступінь, вчене звання, прізвище, ім'я та по-батькові

посада

електронна адреса	телефон	месенджер	консультації

Анотація навчального курсу

Цілі вивчення курсу:	Дисципліна «Безпека інформаційних систем» має на меті розвиток компетенцій в сфері «Безпека в цифровому середовищі» відповідно до Рамки цифрових компетентностей для громадян України.
Результати навчання:	**знати:** - основні загрози і типові вразливості в цифровому середовищі та способи протидії їм; **вміти:** - вибрати найбільш відповідний захист інформаційних систем та цифрового контенту; - дискримінувати ризики та загрози в інформаційних системах; - вибрати найбільш відповідні заходи безпеки та гарантії; - оцінити найбільш підходящі способи належного врахування надійності та конфіденційності; - оцінити найдоцільніші способи використання та обміну особистою інформацією, захищаючи себе та інших від пошкоджень; - оцінити доцільність заяви про політику конфіденційності щодо використання персональних даних у цифрових послугах; - адаптувати найбільш підходящі способи захистити себе від можливих проявів шахрайства та зловживань у цифрових середовищах; - варіювати цифрові технології для захисту прав споживача.
Передумови до початку вивчення:	Базові знання і навички в сфері інформаційних систем та технологій

Мета курсу (набуті компетентності)

Метою курсу є розвиток компетенцій в сфері «Безпека в цифровому середовищі» відповідно до Рамки цифрових компетентностей для громадян України

Знання: знати, аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

Вміння: відповідно до власних потреб та потреб інших людей, а також у складних контекстах, вибрати найбільш відповідний захист пристроїв та цифрового контенту; дискримінувати ризики та загрози в цифрових середовищах; вибрати найбільш відповідні заходи безпеки та гарантії; оцінити найбільш підходящі способи належного врахування надійності та конфіденційності; оцінити найдоцільніші способи використання та обміну особистою інформацією, захищаючи себе та інших від пошкоджень; оцінити доцільність заяви про політику конфіденційності щодо використання персональних даних у цифрових послугах; адаптувати найбільш підходящі способи захистити себе від можливих проявів шахрайства та зловживань у цифрових середовищах; варіювати цифрові технології для захисту прав споживача.

Структура курсу

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
1.	Загальні аспекти захисту інформації.	2/0/0	Загальні аспекти захисту інформації: основні загрози і типові вразливості, оцінка ймовірності реалізації загроз, тяжкості та серйозності відповідних наслідків.	Участь в обговоренні Тести Індивідуальні завдання
2.	Концептуальні засади забезпечення інформаційної безпеки України	2/4/0	Нормативно-правові основи захисту інформації в Україні. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України.	Участь в обговоренні Тести Індивідуальні завдання
3.	Захист пристроїв та безпечне підключення до мережі Інтернет	2/6/0	Захист пристроїв та цифрового контенту, ризики та загрози у цифрових середовищах. Заходи безпеки та захисту, питання надійності та приватності.	Участь в обговоренні Тести Індивідуальні завдання
4.	Захист персональних даних і приватності. Безпека в Інтернеті	2/4/0	Персональні дані та приватність у цифрових середовищах. Використання та обмін інформацією, яка дозволяє встановити особу, зі збереженням можливості захистити себе та інших від шкоди.	Участь в обговоренні Тести Індивідуальні завдання
5.	Захист особистих прав споживача від шахрайства та зловживань	2/4/0	Правові положення щодо захисту мережевого споживача, виявлення сумнівних інтернет-магазинів.	Участь в обговоренні Тести Індивідуальні завдання
6.	Основи криптографії	2/6/0	Основні терміни та поняття. Криптографічні методи захисту інформації. Сучасні криптосистеми та їх особливості. Класичні техніки шифрування. Симетричні та асиметричні алгоритми шифрування інформації. Цифрові підписи. Адміністрування ключами.	Участь в обговоренні Тести Індивідуальні завдання
7.	Програмні віруси та способи їх нейтралізації	2/0/0	Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх	Участь в обговоренні Тести

№	Тема	Години (Л/ЛБ/ПЗ)	Стислий зміст	Інструменти і завдання
			функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети	Індивідуальні завдання

Система оцінювання курсу

Критерії оцінювання та система розподілу балів

Поточний контроль здійснюється лектором. Викладач розробляє чіткі критерії оцінювання всіх видів навчальної роботи у комплексному контролі знань, доводить їх до відома студентів на початку змістовного модулю.

Система оцінювання аудиторної роботи.

Поточна аудиторна діяльність студента оцінюється за чотирибальною (національною) шкалою.

Форми участі студентів у навчальному процесі, які підлягають поточному контролю:

- виступ з основного питання;
- усна доповідь;
- доповнення, запитання до того, хто відповідає, рецензія на виступ;
- участь у дискусіях, інтерактивних формах організації заняття;
- аналіз джерельної та монографічної літератури;
- лабораторні заняття;
- самостійне опрацювання тем;
- підготовка тез, конспектів навчальних або наукових текстів;
- систематичність роботи на семінарських заняттях, активність під час обговорення питань;
- та інші.

Критеріями оцінки є:

1) для усних відповідей:

- повнота розкриття питання;
- логіка викладання, культура мови;
- емоційність та переконаність;
- використання основної та додаткової літератури;
- аналітичні міркування, уміння робити порівняння, висновки ;
- та інші.

2) для виконання письмових завдань:

- повнота розкриття питання;
- цілісність, системність, логічність, уміння формулювати висновки;
- акуратність оформлення письмової роботи
- та інші.

Критерії оцінки рівня знань на практичних/лабораторних заняттях.

На практичних/лабораторних заняттях кожен студент з кожної теми виконує завдання особисто.

Рівень знань оцінюється: ***«відмінно»*** – студент дає вичерпні, обґрунтовані, теоретично і практично правильні відповіді не менш ніж на 90% запитань, рішення задач та вправи є правильними, демонструє знання підручників, посібників, інструкцій, проводить узагальнення і висновки, акуратно оформляє завдання, був присутній на лекціях; ***«добре»–*** коли студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій і розрахунків, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді, був присутній на лекціях, має конспект лекцій чи реферати з основних тем курсу; ***«задовільно»***– коли студент дає правильну відповідь не менше ніж на 60% питань, або на всі запитання дає недостатньо обґрунтовані, невичерпні відповіді, допускає грубі помилки, які виправляє за допомогою викладача. ***«незадовільно з можливістю повторного складання»*** – коли студент дає правильну відповідь не менше ніж на 35% питань, або на всі запитання дає необґрунтовані, невичерпні відповіді, допускає грубі помилки. Підсумкова (загальна оцінка) курсу навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове засвоєння теоретичного матеріалу

Рекомендована література

1. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.
3. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
4. Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.
5. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
6. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510 с.
7. Кузнецов О.О. Захист інформації в інформаційних системах. методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2010.– 316 с.
8. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.
9. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.
10. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.
11. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

Ресурси мережі Internet

1. https://zakon.rada.gov.ua/laws/
2. https://us.norton.com/internetsecurity

Оцінювання курсу

За повністю виконані завдання студент може отримати визначену кількість балів:

Інструменти і завдання	Кількість балів
Участь в обговоренні	20
Тести	20
Індивідуальні завдання/лабораторні роботи	30
Залік	30
Разом	100

Шкала оцінювання студентів

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Політика курсу

Плагіат та академічна доброчесність:	Дотримання академічної доброчесності студентами 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. Порушенням академічної доброчесності вважається: • академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

	• самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів; • фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях; • фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень; • списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання. • За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: • повторне проходження оцінювання (контрольна робота, іспит, залік тощо); • повторне проходження відповідного освітнього компонента освітньої програми.
Завдання і заняття:	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. Всі завдання, передбачені програмою курсу мають бути виконані своєчасно і оцінені в спосіб, зазначений вище.
Поведінка в аудиторії:	На заняття студенти вчасно приходять до аудиторії відповідно до діючого розкладу та обов'язково мають дотримуватися вимог техніки безпеки. Під час занять студенти: – не вживають їжу та жувальну гумку; – не залишають аудиторію без дозволу викладача; – не заважають викладачу проводити заняття. Під час контролю знань студенти: – є підготовленими відповідно до вимог даного курсу; – розраховують тільки на власні знання (не шукають інші джерела інформації або «допомоги» інших осіб); – не заважають іншим; – виконують усі вимоги викладачів щодо контролю знань.