Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра інформаційних технологій та систем електронних комунікацій

СИЛАБУС

навчальної дисципліни «Безпека інформаційно-комунікаційних систем»

1. Загальна інформація

Назва дисципліни	Безпека інформаційно-комунікаційних систем
Статус дисципліни	Вибіркова
Рівень вищої освіти, форма навчання	другий(магістерський), денна форма
Освітньо-професійна програма	Комп'ютерні науки
Спеціальність	122 Комп'ютерні науки
Рік навчання, семестр	2-й рік (3 семестр)
Мова викладання	українська
Викладач	Бурак Назарій Євгенович, к. т. н., доцент, заступник начальника кафедри інформаційних технологій та систем електронних комунікацій
E-mail	**n.burak@ldubgd.edu.ua,**
Сторінка курсу в ВУ	**http://virt.ldubgd.edu.ua/course/view.php?id=692**
Консультації	Згідно розкладу консультацій кафедри і інформаційних технологій та систем електронних комунікацій

2. Анотація до курсу

Освітня програма підготовки магістра зі спеціальності «Комп'ютерні науки» передбачає підготовку фахівців, здатних розробляти, впроваджувати та супроводжувати інформаційні технології та системи, знаходити раціональні методи та засоби розв’язку задач, забезпечувати сталий розвиток ІТ-компаній, вирішувати прикладні і наукові завдання в області комп’ютерних наук та інформаційних технологій.

Курс "Безпека інформаційно-комунікаційних систем" входить до складу блоку освітніх компонент №2 (Мейджор 2) «Адміністрування комп’ютерних систем (DevOps-інженерія)» та за своїм інформаційним наповненням, має широкий міждисциплінарних зв'язків, формуючи компетенції, необхідня при реалізації різних ІТ проектів.

Предметом вивчення навчальної дисципліни є основні терміни, поняття та визначення в галузі безпеки інформаційно-комунікаційних системах, моделі загроз та сучасні методи, механізми та сервіси захисту інформації, особливості забезпечення конфіденційності та цілісності даних в

інформаційних системах, безпека у розподілених системах, апаратні та програмні складові систем захисту, принципи роботи відкритих ключів та їх сертифікати.

Інструментальними засобами для оволодіння предметом вивчення навчальної дисципліни є середовище віртуального моделювання та симуляції роботи мережі Cisco Packet Tracer, програмне забезпечення Tcp Port Scanner та RedEyes Host Monitor.

3. Мета і завдання курсу

3.1. Метою вивчення дисципліни «Безпека інформаційно-комунікаційних систем» є розкриття сучасних концепцій, технологій та методів забезпечення безпеки інформації в системах електронних комунікацій та формування у здобувачів вищої освіти знань щодо: проблем уразливості інформації в сучасних мережавх обміну інформацією; методології захисту інформації; засобами технічного, апаратного та програмного захисту, а також захищеними технологіями електронних комунікаційних систем; методами перевірки цілісності об'єктів і суб'єктів інформаційної діяльності; особливостей організації захисту інформації на об'єктах інформаційної діяльності.

3.2. Завдання:

- засвоєння теоретичних основ процесу забезпечення безпеки інформації в інформаційно-комунікаційних системах;
- формування у здобувачів освіти компетенції з використання сучасних методів та засобів захисту інформаційних ресурсів;
- отримання знань, вмінь та навичок реалізації процесів захисту даних в розподілених інформаційно-комунікаційних системах.

3.3. Компетентності:

Загальні компетентності:

- Здатність, вчитися і оволодівати сучасними знаннями.
- Здатність застосовувати знання у практичних ситуаціях.
- Здатність генерувати нові ідеї (креативність).

Спеціальні (фахові) компетентності:

- СК10 Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення
- СК11 Здатність ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп'ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом.

3.4. Програмні результати навчання:

- РН6 Розробляти концептуальну модель інформаційної або комп'ютерної системи.
- РН10 Проектувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

4. Формат і обсяг курсу

Формат курсу Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох змістових модулів, які є логічно завершеними, відносно самостійними, цілісними частинами. Засвоєння теоретичного матеріалу курсу передбачає відвідування 8 лекційних занять, здачу тестових завдань на базі електронного освітнього середовища (до кожної лекції) та виконання практичних робіт.

Освоєння практичної частини курсу зосереджено в рамках 8 практичних занять, під час яких здобувачам освіти нобхідно виконати 7 практичних робіт. Виконані роботи необхідно завантажувати до відповідної категорії електронного освітнього середовища для їх подальшого захисту на оцінку.

Обсяг дисципліни: 4,5 кредити / 135 академічних годин, з яких: лекцій 16 годин, практичних 16 години, самостійної роботи 103 години.

Форми навчання лекції, практичні заняття, консультації, самостійна робота.

5. Тематика та зміст курсу

Назви змістових модулів і тем	Кількість годин				
	усього	у тому числі			
		л	п	лаб	с.р.
1	2	3	4	5	6
Змістовний модуль 1. ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ.					
Тема 1.1. Вступ до предмету. Основні поняття.	10	2			8
Тема 1.2. Базові системи захисту.	22	2	4		16
Тема 1.3. Типові вразливості систем та причини їх появи.	16	2	2		12
Тема 1.4. Шкідливе програмне забезпечення.	18	2	2		14
Усього годин за змістовим модулем 1	**66**	**8**	**8**		**50**
Змістовний модуль 2. ЗАХИСТ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ.					
Тема 2.1. Основи безпеки інформації в комп‘ютерних мережах	16	2	2		12
Тема 2.2. Засоби захисту в розподілених інформаційно-комунікаційних системах.	20	2	2		16
Тема 2.3. Безпека мережевих протоколів Internet.	17	2	2		13
Тема 2.4. Передавання інформації захищеними мережами.	16	2	2		12
Усього годин за змістовим модулем 2	**69**	**8**	**8**		**53**
Усього годин	**135**	**16**	**16**		**103**

6. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Основи захисту інформації в інформаційно-комунікаційних системах.

Тема 1.1. Вступ до предмету. Основні поняття.

Вступ. Термінологія. Завдання захисту та загрози безпеці інформації. Класифікація атак. Модель загроз та модель порушника.

Тема 1.2. Базові системи захисту.

Архітектура та рівні інформаційно-комунікаційної системи. Функціональні сервіси безпеки та їх механізми. Основні підсистеми комплексу засобів захисту. Моделювання структури захисту інфомраційних систем.

Тема 1.3. Типові вразливості систем та причини їх появи.

Передумови виникнення вразливостей в інформаційно-комунікаційних системах. Класифікація вад безпеки. Помилки програмної реалізації систем: переповнення буфета та оброблення текстових рядків. Люки.

Тема 1.4. Шкідливе програмне забезпечення.

Класифікація шкідливого програмного забезпечення. Методи виявлення та протидії. Засоби аналізу захищеності та цілісності системи.

Змістовий модуль 2. Захист розподілених інформаційно-комунікаційних систем.

Тема 2.1. Основи безпеки інформації в комп‘ютерних мережах

Основні відомості про комп‘ютерні мережі. Загрози безпеці інформації у мережах. Безпека взаємодії відкритих систем.

Тема 2.2. Засоби захисту в розподілених інформаційно-комунікаційних системах.

Архітектура захищених мереж. Міжмережні екрани. Системи виявлення атак. Системи аналізу та оцінювання вразливостей.

Тема 2.3. Безпека мережевих протоколів Internet.

Протоколи прикладного рівня. Транспортні протоколи. Протоколи IP. Протоколи керування мережею.

Тема 2.4. Передавання інформації захищеними мережами.

Захист інформації у відкритих канал зв‘язку. Віртуальні захищені мережі. Рівні реалізації віртуальних захищених мереж. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні. Електронний цифровий підпис

7. Завдання для самостійного опрацювання

1. З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні практичні завдання, які отримують в під час практичних заняття. Зміст та варіанти виконання практичних завдань (методичні рекомендації) відображені на платформі електронного освітнього середовища «Віртуальний університет». Звіт про виконання індивідуальних практичних завдань завантажується у відповідну категорію електронного освітнього середовища для подальшої перевірки викладачем та його захисту на оцінку.

8. Методи навчання

Основні форми організації навчання: лекції; практичні заняття з проведенням зрізів знань; індивідуальні практичні завдання, консультації.

Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та пояснювально-ілюстративний (наочний) метод (демонстрація, ілюстрація);
- практичні роботи – дослідницький метод (метод спостереження), репродуктивний метод (відтворення алгоритму та структури запитів згідно заданих критеріїв),
- індивідуальні практичні завдання – частково-пошуковий метод навчання (певні елементи матеріалу відомі, решту здобувачі освіти отримують самостійно виконуючи завдання, розв’язуючи задачі тощо);
- консультації – словесний та дискусійний методи.

9. Технічне й програмне забезпечення /обладнання

Комп'ютери на базі процесорів Intel Pentium Gold G5400, компоненти програмного забезпечення MS Office 365 (Word, Excel, PowerPoint), інтерактивна система управління комп'ютерами Veyon; програмне забезпечення: інтерактивне середовище Cisco Packet Tracer (вільне програмне забезпечення), Tcp Port Scanner (вільне програмне забезпечення), RedEyes Host Monitor (вільне програмне забезпечення).

10. Критерії оцінювання

Оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до «Положення про організацію освітнього процесу у ЛДУ БЖД» https://cutt.ly/0WRAkEh та «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД» https://cutt.ly/iWRAWF3.

Поточний контроль

Поточний контроль проводитися у формі виконання тестових завдань на базі платформи електронного освітнього середовища «Віртуальний університет» та виконання індивідуальних практичних завдань та їх захисту на оцінку. Оцінювання результатів поточного контролю здійснюється за національною (чотирибальною) шкалою. Результати поточного контролю (поточна успішність) враховуються викладачем при визначені допуску до підсумкового контролю та виставленні підсумкової оцінки за диференційований залік.

Вид робіт	**Формат проведення та критерії оцінювання**
Тестові завдання	Курсом передбачено проходження 8 тестових завдань. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 40 балів. Також передбачено одне підсумкове тестування за матеріалами цілого курсу, яке оцінюється в 20 балів.
Робота на практичному занятті; Індивідуальні практичні завдання	Курсом передбачено виконання та захист 8-х індивідуальних практичних робіт. Оцінювання здійснюється за національною (чотирибальною) шкалою, відповідно до Додатку Б «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД». За успішне виконання практичних завдань сумарно можна отримати до 40 балів.

За виконання завдань та тестувань здобувач може отримати до **100** балів

Підсумковий контроль

Семестровий контроль проводиться у формі диференційованого заліку. Допуск до семестрового контролю здійснюється за умови виконання здобувачем індивідуальних практичних і тестових завдань та одержання понад **60** зі **100** можливих балів за результатами проходження курсу на базі віртуального навчального середовища.

Диференційований залік **(максимально 50 балів)** складається із двох компонентів: тестування у електронному освітньому середовищі "Віртуальний університет" (максимум 30 балів) та розв'язуванні одного типового практичного завдання (максимум 20 балів), яке оцінюється:

Практичне завдання (20 балів)

- 16-20 балів – виконано розв'язання запропонованої практичної задачі у повні мірі;
- 11-15 балів – розв'язання запропонованої практичної задачі не в повній мірі;

- 6-10 балів – наведене розв'язання запропонованої практичної задачі містить неточності або не відповідають змісту завдання, проте містить помилки або не враховує усі особливості реалізації;
- 1-5 балів – розв'язання запропонованої практичної задачі не вірне або відсутнє, однак спостерігається вірно обраний напрям вирішення завдання;
- 0 балів – завдання не виконане або розв'язок не відповідає поставленому завданню.

Підсумкова семестрова оцінка обчислюється як сума балів поточного (з коефіцієнтом 0,5 з округленням до цілого числа) та підсумкового контролю за 100-бальною шкалою і переводяться в національну (чотирибальну) шкалу (“відмінно”, “добре”, “задовільно”, “незадовільно”).

Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості, залікової книжки (позитивні результати) здобувача в національній, 100-бальній шкалі та шкалі ЄКТС відповідно до співвідношень, поданих у наступній таблиці.

Шкала оцінювання результатів навчання здобувачів вищої освіти

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, диференційованого заліку, курсового проекту (роботи), практики	для заліку
91 – 100	**A**	відмінно	зараховано
81-90	**B**	добре	
71-80	**C**		
61-70	**D**	задовільно	
51-60	**E**		
36-50	**FX**	незадовільно	не зараховано
0-35	**F**		

11. Політика курсу

Виконання навчальних завдань і робота в курсі має відповідати вимогам «Кодекс академічної доброчесності та корпоративної культури ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/kodeks_akademichnoyi_dobrochesnosti_ta_korpo.pdf

Академічні очікування від здобувачів – своєчасне виконання тестових завдань, передбачених силабусом дисципліни; обов’язкове відвідування практичних занять і виконання ідивідуальних практичних робіт(завдань самостійної роботи).

Політика щодо термінів виконання завдань та ліквідації академічної заборгованості: терміни виконання завдань вказуються у електронному курсі «Віртуального університету». Після завершення терміну прийому завдань, система блокує можливість їх завантаження для подальшої оцінки викладачем, окрім випадків пов’язаних із поважними причинами, про що здобувач особисто повідомляє викладача. Відпрацювання академічної заборгованості з дисципліни можливо до дня проведення підсумкового контролю (відповідно до розкладу).

Недопущені до підсумкового контролю здобувачі освіти здійснюють перездачу в терміни, відведені для усунення академічної заборгованості у два етапи:

заборгованість із поточного контролю;

заборгованість із підсумкового контролю.

Ліквідація заборгованості поточного контролю відбувається шляхом проходження тестових завдань та виконання індивідуальних практичних завдань згідно із тематичним планом курсу. Ліквідація заборгованості з підсумкового контролю організовується в форматі перездачі диференційованого заліку.

Дотримання принципів академічної доброчесності: роботи (завдання) виконуються здобувачами самостійно, ідеї та ініціативи інших авторів використовуються лише при належно оформленному цитуванні.

Поведінка в аудиторії – неприпустимо запізнення та користування телефоном на заняттях, за винятком виконання громіздких обчисленнях та використанні додаткових програм в освітніх цілях; повага до думки інших колег; дотримання норм культури мовлення та ін.

12. Рекомендована література

12.1. Основна:

1. *Гайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.
2. *Сенів М. М.* Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с
3. *Юдін О.К., Корченко О.Г., Конахович В.Г.* Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
4. *Лаптєв О.А.* Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навчальний посібник / О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. – К.: ДУТ, 2020. – 126 с.
5. *Ластівка Г.І.* Технічний захист інформації в інформаційних та телекомунікаційних системах: навчальний посібник / Г.І. Ластівка, П.М. Шпатар. Чернівці, Чернівецький національний університет, 2018. – 252 с.

12.2. Додаткова:

1. *Качинський А.Б. Б*езпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К.: 2004. – 472 с.
2. *Бурячок В.Л.* Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.
3. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с
4. *Хорошко В. О.* Проєктування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць/ Львів : Видавництво Львівської політехніки, 2020. – 320 с.
5. *Кузнецов О.О.* Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.
6. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник [та ін.]. Львів : Вид-во. Львівської політехніки, 2019. – 580 с.
7. *Богуш В.М.* Основи кіберпростору, кібербезпеки та кіберзахисту: Навч.посіб. /В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін – К. : Ліра-К, 2020. – 554 с.
8. *Eugene H. Spafford.* The Internet Worm Program: An Analysis // Purdue Technical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.
9. *Stallings W.* Data and Computer Communications 10th - Pearson, 2013. – 912 p.
10. Указ Президента України від 25 лютого 2017 року N47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»». Президент України.URL: https://www.president.gov.ua/documents/472017-21374

12.3. Інформаційні ресурси:

1. *Віртуальний університет ЛДУ БЖД* [Електронний ресурс]. — Доступний з http://virt.ldubgd.edu.ua/
2. *Cyber Security Training. SANS Institute.* Онлайн курси із захисту інформації. [Електронний ресурс]. – Доступний з http://www.sans.org
3. *Інформаційний онлайн-журнал Infosecurity* [Електронний ресурс]. – Доступний з https://www.infosecurity-magazine.com/

Розглянуто на засіданні кафедри інформаційних технологій та систем електронних комунікацій протокол від «30» _серпня_ 2023 року №_1_

РОЗРОБНИК
Заступникначальника кафедри інформаційних технологій та систем електронних комунікацій
кандидат технічних наук, доцент

_____ Назарій БУРАК
«_30_» _серпня_ 2023 р.

ЗАТВЕРДЖЕНО
Начальник кафедри інформаційних технологій та систем електронних комунікацій
кандидат технічних наук, доцент

_____ Олександр ПРИДАТКО
«_30_» _серпня_ 2023 р.

ПОГОДЖЕНО
Гарант освітньої програми «Комп'ютерні науки» другого (магістерського) рівня вищої освіти
кандидат технічних наук, доцент

_____ Назарій БУРАК
«_30_» _серпня_ 2023 р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту
кандидат фізико-математичних наук, доцент

_____ Ольга МЕНЬШИКОВА
«_30_» _серпня_ 2023 р.

Дата актуалізації*					
Підпис					
Ім’я, прізвище завідувача кафедри					