СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Лектор курсу			**Гайдур Галина Іванівна**, завідувач кафедри Інформаційної та кібернетичної безпеки Алексенко Сергій Олександрович Асистент кафедри Інформаційної та кібернетичної безпеки		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail**: ikbdut@gmail.com; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=1195	
Галузь знань			12 «Інформаційні технології»		**Рівень вищої освіти**	бакалавр	
Спеціальність			126 Інформаційні системи та технології		**Семестр**	7	
Освітня програма			Інформаційні системи та технології		**Тип дисципліни**	Обов'язкова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	–	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	Отримання теоретичних знань і практичних навичок щодо забезпечення кібербезпеки в інформаційно-комунікаційних системах

Освітні компоненти, які передують вивченню	Програмування мобільних пристроїв, Інформаційні мережі
Освітні компоненти для яких є базовою	Кваліфікаційна робота. Підсумкова атестація

Компетентності відповідно до освітньої програми

Soft-skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу. КЗ 2. Здатність застосовувати знання у практичних ситуаціях. КЗ 3. Здатність до розуміння предметної області та професійної діяльності. КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.	КС 1. Здатність аналізувати об'єкт проектування або функціонування та його предметну область. КС 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем,

КЗ 7. Здатність розробляти та управляти проектами. КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт	продуктів, сервісів і елементів інфраструктури організації. КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем. КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків. КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації. КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет). КС 14. Здатність формувати нові конкурентоспроможні ідеї й реалізовувати їх у проектах (стартапах)

Програмні результати навчання (ПРН)

ПР 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.
ПР 9. Здійснювати системний аналіз архітектури підприємства та його ІТ-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. ***Основи побудови комплексу засобів захисту для інформаційно-комунікаційних систем.*** ***Знати***: теоретичні основи побудови КЗЗ для ІКС. Модель порушника. Основні положення вітчизняної та міжнародної нормативної бази щодо безпеки інформації. ***Вміти:*** володіти основами комплексного забезпечення ІБ ІКС та принципами її побудови. Використовувати типові методи та засоби вирішення проблеми комплексного забезпечення ІБ в ІКС. Володіти основами формування політик ІБ щодо ІКС. ***Формування* компетенцій**: КЗ1, КЗ2, КЗ3, КЗ5, КЗ7, КЗ8, КС1,	Лекція 1	5,5*	Лекція-візуалізація
			Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 1		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни

КС2, КС5, КС6, КС12, КС14 ***Результати навчання:*** ПР6, ПР9 ***Рекомендовані джерела:*** 1-4			Ділова гра
Тема 2. ***Механізми та засоби захисту операційних систем Windows та UNIX.*** ***Знати***: особливості забезпечення безпеки ресурсів ОС Windows та UNIX. Підходи та методи щодо створення захищених ОС. Знання технологій TCP/IP, DNS, DHCP, SSL/TLS. ***Вміти***: використовувати типові підходи щодо створення захищених ОС. Виконувати адміністрування ОС. Реалізувати основні методи захисту ОС. ***Формування компетенцій:*** К31, К32, К33, К35, К37, К38, КС1, КС2, КС5, КС6, КС12, КС10, КС14 ***Результати навчання:*** ПР6, ПР9 ***Рекомендовані джерела:*** 1, 3-6	Лекція 2	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Лекція 3		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 2		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
			Тестування, навчальна дискусія, кейс-метод
Тема 3. ***Механізми та засоби захисту СУБД.*** ***Знати***: основи безпеки та методи реалізації засобів захисту інформації в СУБД Access, MS SQL Server, Oracle. ***Вміти***: застосовувати систему безпеки СУБД Access, MS SQL Server, MySQL. Реалізувати управління параметрами безпеки. ***Формування компетенцій:*** К31, К32, К33, К35, К37, К38, КС1, КС2, КС5, КС6, КС12, КС10, КС14 ***Результати навчання:*** ПР6, ПР9 ***Рекомендовані джерела:*** 1, 3-6	Лекція 4	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Лекція 5		Мозковий шторм, навчальна дискусія, вирішення практичних задач
	Практичне заняття 4		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 5		Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
			Проведення модульного контролю № 1
Тема 1. Основи побудови комплексу засобів захисту для інформаційно-телекомунікаційних систем та мереж. **Тема 2.** Механізми та засоби захисту операційних систем Windows та UNIX. **Тема 3**. Механізми та засоби захисту СУБД.	Самостійна робота		1. Безпека інформаційної технології та її значення у сучасному суспільстві. Теоретичні засади, напрями розвитку. 2. Поняття про політику та послуги безпеки, механізми захисту, засоби та КЗЗ. 3. Принципи розробки програмних засобів зламу парольного

			захисту. 4. Технології TCP/IP, DNS, DHCP, SSL/TLS. 5. Сучасні підходи до створення захищених ОС. 6. Характеристика системи управління доступом в ОС Windows. 7. Основи адміністрування ОС, протоколи передачі інформації, способи захисту інформації в мережі. 8. Локальна політика безпеки параметрів ОС Windows. 9. Групова політика ОС Windows. 10. Забезпечення безпеки ресурсів ОС Windows/UNIX. 11. Основи забезпечення захисту ОС на прикладі ОС Linux.
Тема 4. ***Механізми та засоби захисту від шкідливих програмних засобів.*** ***Знати:*** основні класи шкідливих програмних засобів, їх властивості. Методи, заходи, функції та можливості сучасних антивірусних програм (AVP). Види ПРП. ***Вміти***: експлуатувати методи та засоби захисту програм і даних від ШП засобів. Проводити оцінку ефективності сучасних AVP. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ3, КЗ5, КЗ7, КЗ8, КС1, КС2, КС5, КС6, КС12, КС10, КС14 ***Результати навчання:*** ПР6, ПР9 ***Рекомендовані джерела:*** 1, 3-6.	Лекція 6	5,5*	Лекція-візуалізація, експрес-опитування студентів
			Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 6		Лекція-візуалізація, експрес-опитування студентів
			Тестування, навчальна дискусія, вирішення практичних задач
			Ділова гра, вирішення практичних задач
Тема 5. ***Механізми та засоби захисту комп'ютерних мереж.*** ***Знати:*** принципи дії, реалізацію програмно-апаратних засобів захисту інформації в комп'ютерних мережах (КМ). Загрози типу DoS/DDoS. Структуру, функції та методи реалізації засобів захисту інформації (ЗЗІ) від Spam. ***Вміти***:характеризувати побудову та реалізацію ЗЗІ в КМ. Обґрунтовувати раціональні шляхи і засоби протидії DoS/DDoS. Експлуатувати ефективну СЗІ від розповсюдження спаму. ***Формування компетенцій:*** КЗ1, КЗ2, КЗ3, КЗ5, КЗ7, КЗ8, КС1, КС2, КС5, КС6, КС12, КС10, КС14 ***Результати навчання:*** ПР6, ПР9 ***Рекомендовані джерела:*** 1, 3-6.	Лекція 7	5,5*	Лекція-візуалізація, експрес-опитування студентів
			Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни
	Практичне заняття 7		Тестування, навчальна дискусія, вирішення практичних задач
			Тестування, навчальна дискусія, вирішення практичних задач

<table>
<tr><td rowspan="4">Тема 6. Перспективні напрями розвитку комплексу засобів захисту (КЗЗ) інформації в розподілених середовищах.
<u>Знати:</u> основні характеристики систем аналізу уразливостей та виявлення вторгнень. Сучасні засоби СВВ провідних виробників. Типові методи та засоби вирішення ЗІ щодо сучасних мобільних пристроїв провідних виробників.

<u>Вміти</u>: використовувати новітні технології засобів захисту мобільних пристроїв провідних виробників.
<u>Формування компетенцій:</u> ЗК1, ЗК2, ЗК4, ЗК6, ЗК7, ЗК15
<u>Результати навчання:</u> ПР6, ПР9
<u>Рекомендовані джерела:</u> 1, 3-6.</td><td>Лекція 8</td><td rowspan="4">5,5*</td><td>Лекція-візуалізація, експрес-опитування студентів</td></tr>
<tr><td>Лекція 9</td><td>Тестування, навчальна дискусія, вирішення практичних задач</td></tr>
<tr><td>Практичне заняття 8</td><td>Усне опитування, навчальна дискусія, доповідь з презентацією за тематикою самостійного вивчення дисципліни</td></tr>
<tr><td>Практичне заняття 9</td><td>Проведення модульного контролю №2.</td></tr>
<tr><td>Тема 4. Механізми та засоби захисту від шкідливих програмних засобів.
Тема 5. Механізми та засоби захисту комп’ютерних мереж.
Тема 6. Перспективні напрями розвитку комплексу засобів захисту (КЗЗ) інформації в розподілених середовищах.</td><td>Самостійна робота</td><td></td><td>1. Поняття про threat analysis, malware analysis.
2. Сучасні технології для оперативного дослідження актуальних проблем інформаційної безпеки.
3. IBM X-Force Threat Intelligence. Можливості та напрями роботи.
4. Модель Computer viruses та модель Trojan horse.
5. Petya/NotPetya/Petya.A.
6. Мережеві черв’яки Duqu, Flame та Stuxnet.
7. Використання блоку емпіричного розпізнавання Computer viruses в антивірусних програмах.
8. Виявлення, блокування та знищення Keyloggers.
9. Системи класу EPP та EDR для розширеного виявлення і реагування на знайдені складні загрози. Призначення та можливості.
10. Порівняльна характеристика постачальників сучасних EPP рішень щодо захисту кінцевих пристроїв від ESET, Symantec, Sophos, Trend Micro.
11. Основні типи засобів забезпечення ІБ в комп’ютерних мережах.
12. Стандарти IPSec. Модель TCP/IP.
13. XSS-attack; SQL-injection; Buffer Overflow.
14. NGFW основних світових виробників.
15. Визначення стійкості Web-серверу.
16. Настройка параметрів доступу користувачів Internet до ресурсів внутрішньої мережі.</td></tr>
<tr><td colspan="4">МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ</td></tr>
</table>

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять;
- Програмно-апаратний комплекс системою управління подіями та інцидентами кібербезпеки IBM Security QRadar SIEM;
- Програмний комплекс виявлення вразливостей веб-додатків та веб-сервісів, Nessus;
- Програмний комплекс Security Management Center ESET.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с. URL: http://www.dut.edu.ua/uploads/p_303_92597962.pdf
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf
3. Ю.А.Тарнавський Технології захисту інформації [Підручник] / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. URL: http://www.dut.edu.ua/uploads/l_1885_83261529.pdf
4. Social Engineering: The Science of Human Hacking Published by John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, . – 362 p. –IN 46256 URL: http://www.dut.edu.ua/uploads/l_2112_74001205.pdf
5. Shin Bongsik. A Practical Introduction to Enterprise Network and Security Management CRC Press Taylor & Francis Group, 2017. — 614 p. — ISBN 978-750-8400. URL: http://www.dut.edu.ua/ua/lib/1/category/96/view/2139
6. Waschke Marvin. Personal Cybersecurity: How to Avoid and Recover from Cybercrime. Personal Cybersecurity, Apress, 2017. – 240 p. – ISIN 978-1484224298. URL: http://www.dut.edu.ua/ua/lib/1/category/96/view/2140

ПОЛІТИКА КУРСУ

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ	***Робота на заняттях,*** *у т.ч.:*	

КОНТРОЛЬ	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1	максимальна оцінка – 15 балів
	Модульний контроль № 2	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни впрактичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82 - 89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих	**Достатній** Забезпечує студенту самостійне вирішення	Добре / Зараховано (В)

	ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не*

			проставляється