Приватне акціонерне товариство
«Приватний вищий навчальний заклад
«Запорізький інститут економіки та інформаційних технологій»

Кафедра економічної кібернетики та інженерії програмного забезпечення

"**ЗАТВЕРДЖУЮ**"
Проректор з навчальної роботи
_____ Д.Є.Швець
"_30_" _серпня_ 2021 року

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК 27 Безпека програм та даних

Освітньо-професійна програма__Інженерія програмного забезпечення____
(назва ОПП)

спеціальності: 121 «Інженерія програмного забезпечення»

спеціалізація_____
(назва спеціалізації при наявності)

Рівень вищої освіти: перший (бакалаврський)

2021 – 2022 навчальний рік

Мова викладання: українська

Прізвище, ім'я та по-батькові викладача/розробника:
Домашев Геннадій Євгенович к.т.н.

Електронна адреса викладача_____

Дні занять за розкладом згідно з розкладом

Графік консультацій (он-лайн консультації)_____субота_____

Сторінка курсу в Moodle: http://moodle.zieit.zp.ua/course/view.php?id=1359

Силабус схвалено на засіданні кафедри
економічної кібернетики та
інженерії програмного забезпечення

Протокол від «30» серпня 2021 року № 1

Завідувач кафедри ЕКІПЗ
_____ (Явтушенко С.О.)
(підпис) (прізвище та ініціали)

Силабус погоджено
Начальник навчального відділу
_____О.В.Сташкевічус

1. Опис дисципліни

Анотація дисципліни (Призначення навчальної дисципліни)	Дисципліна надає, студентам знання, щодо сучасних стандартів, підходів, методів та засобів захисту програм та даних. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від несанкціонованого копіювання, захисту програмних засобів від дослідження.
Мета вивчення	Оволодіння теоретичними знаннями та засвоєння практичних навичок.
Завдання навчальної дисципліни	Отримання студентом компетенції для того, щоб приймати участь у проектуванні інформаційних систем, розглянуті загальні питання криптоаналізу, зокрема типи криптоаналізу з точки зору інформації, яку має криптоаналітик; надана класифікація шифросистем стосовно захищеності (стійкості до криптоаналізу). Наведені приклади зламування шифросистем. Значна увага приділяється електронному цифровому підпису, який підтверджує дійсність і цілісність документа та засвідчує авторство. Реалізації дискретних структур різних типів, створення складних процедур обробки.
Пререквізити	1. «Вища математика»; 2. «Теорія ймовірностей та математична статистика», 3. «Комп'ютерна дискретна математика»; 4. «Серверні операційні системи».
Результати навчання	1. Здатність діяти соціально відповідально та свідомо. 2. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). 3. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. 4. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем. **Програмні результати навчання:** ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення. ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем. ПР26. Вміти використовувати сучасні технології та інструментальні засоби для проектування і розробки WEB-додатків.

2. Обсяг та ознаки навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна та дистанційна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="8">Галузь знань:
12 «Інформаційні технології»

Спеціальності:
121 «Інженерія програмного забезпечення»

_____

Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 1</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання - не передбачено</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="6">Загальна кількість годин – 120</td><td>7-й</td><td>7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td colspan="2">-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>80 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">0 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

3. Дидактична карта дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі				бали	усього	у тому числі				
		л	п	інд.	с.р.			л	п	інд.	с.р.	бали
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1.												
Тема 1: Актуальність проблеми забезпечення безпеки програм та даних.	30	6	4		20	15	30	1	1		22	15
Тема 2. Базова модель безпеки	30	4	4		20	15	30	1	1		26	15
Тема 3. Основні механізми розгортання операційної системи (які застосовуються для ОС Microsoft). Забезпечення безпеки зберігання даних в операційній системі Microsoft.	30	4	4		20	15	30	2	2		30	15
Тема 4. Криптографічні засоби захисту інформації	30	6	8		20	15	30	2	2		30	15
Разом за змістовим модулем 1	120	20	20		80	60	120	6	6		108	60
ІНДЗ			-	-		-			-	-	-	
Усього годин	120	20	20		80	60	120	6	6		108	60

4. Самостійна робота

№ з/п	Тема та зміст	Кількість годин
1	Тема 1. Сервіси і механізми захисту	8/12
2	Тема 2. Принципи побудови блочних шифрів та криптосистем з відкритим ключем	8/12
3	Тема 3. Сучасні алгоритми симетричного та асиметричного шифрування	8/11
4	Тема 4. Сучасні алгоритми хешування	8/11

5	Тема 5. Основні методи безпечного написання коду програм	8/10
6	Тема 6. Методи і засоби аналізу безпеки програмних засобів	8/11
7	Тема 7. Використовувати функції Microsoft CryptoAPI для розробки прикладного ПЗ	8/10
8	Тема 8. Протоколи автентифікації	8/10
9	Тема 9. Програмна реалізація криптографічних алгоритмів	8/11
10	Тема 10. Методи безпечної реалізації ПЗ	8/10
Разом		80/108

Самостійна робота студентів з дисципліни “Безпека програм та даних” складається з:

- опрацювання теоретичних питань дисципліни (першоджерел та навчально-методичної літератури);
- підготовка до лабораторних занять та складання звітів до лабораторних робіт.

4. Індивідуальні завдання

Відсутні.

5. Методи навчання

- Словесні (пояснення, розповідь, лекція, бесіда), наочні (ілюстрація, демонстрація), практичні вправи.
- Індуктивні (вивчення явищ від одиничного до загального), дедуктивні (вивчення явищ від загального окремого).
- Проблемно-пошукові, дослідницькі, евристичні, аналітичні.

6. Система контролю та оцінювання.

Передбачається три форми контролю засвоєння дисципліни: поточний, модульний та підсумковий. Система контролю залежить від форми проведення занять. Зокрема, на лекціях передбачено:

- фронтальне опитування;
- вибіркове усне опитування;
- письмове опитування;
- тестування;
- технічний диктант.

На практичних заняттях:

- тестування;
- комбіноване опитування;
- письмове опитування за індивідуальним завданням;
- усне опитування за індивідуальним завданням;
- програмоване опитування;
- взаємоконтроль;
- співбесіда;
- контрольна робота;
- захист лабораторних робіт.

По результатам виконання самостійної роботи студентів:

- перевірка конспекту;
- перевірка відповідей на проблемні питання;
- перевірка ІДЗ.

Модульний контроль проводиться у формі комп'ютерного тестування в спеціалізованій тестовій системі (Moodle). Тривалість складання студентом тестів модульної контрольної роботи не перевищує однієї академічної години. Максимальний рейтинговий бал при цьому не перевищує 40 балів.

Підсумковим контролем засвоєння дисципліни є іспит. У відповідності до стандарту підприємства підсумковий контроль автоматично проставляється як сума рейтингових балів поточного та модульного контролю. У разі недостатньої кількості балів (<60) та мінімально необхідної кількості балів поточного контролю (від 20 балів) студент має змогу здавати екзамен у письмовій формі за екзаменаційними білетами, що розроблені викладачем, згідно за розробленим навчальним відділом розкладом. Письмову роботу кодують та надають викладачу на перевірку. Кількість максимальних рейтингових балів становить 40. Ці бали замінюють рейтингові бали модульного контролю, та у разі достатньої кількості з поточним контролем ставиться оцінка. Кількість спроб складання іспиту не перевищує трьох.

7. Технічне й програмне забезпечення/обладнання.

Лабораторний практикум з дисципліни «Безпека програм та даних» проводиться у спеціально обладнаних комп'ютерних аудиторіях. Робочі місця користувачів обладнані комп'ютерами достатньої потужності з постійним підключенням до мережі Internet.

Політики безпеки передбачають роботу користувачів у складі домену з обов'язковою авторизацією та виділенням мережевих дискових квот для зберігання основних результатів роботи.

Всі матеріали, необхідні студентам для успішного засвоєння дисципліни (методичні вказівки, спеціалізоване програмне забезпечення, основна та додаткова література, а також результати проходження етапів вивчення курсу доступні у внутрішній учбовій мережі на файловому сервері.

Самостійна робота може виконуватись як в лабораторіях ЗІЕІТ, так і у інших зручних місцях для студента, у час, вільний від основного навчання, та за умови наявності у нього персонального комп'ютера з відповідним програмним забезпеченням.

Перелік необхідного програмного забезпечення:

- довільна операційна система, що дозволяє підключатися до мережі;
- будь-яке програмне забезпечення, що дозволяє працювати з файлами документів найбільш розповсюджених форматів;

Все програмне забезпечення має бути вільного користування або з відповідною ліцензією чи умовами (наприклад учнівська, тимчасова та ін.)

8. Політика дисципліни.

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. Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.

Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в дистанційному режимі за погодженням із деканатом та керівником курсу. В такому випадку виконані завдання презентуються під час консультації викладача.

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, а також виконання завдань з метою закріплення теоретичного матеріалу.

За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент отримує за заняття 0 балів і зобов'язаний відпрацювати таке заняття.

Ліквідація заборгованості відбувається протягом 1 тижня після встановленого терміну. При цьому оцінка знижується на 10 %.

Здобувачам вищої освіти після аудиторних занять надається право підвищувати свій рейтинг лише під час складання іспитів (підсумкового оцінювання) за графіком екзаменаційної сесії.

У разі виявлення факту плагіату студент отримує за завдання 0 балів і повинен повторно виконати завдання, які передбачені у силабусі.

Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування.

9. Розподіл балів, які отримують студенти

<table>
<tr><td colspan="4">Поточне тестування та самостійна робота</td><td>Сума</td></tr>
<tr><td colspan="4">Змістовий модуль</td><td>Підсумкова робота (МК, залік)</td><td rowspan="3">100</td></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td><td rowspan="2">40</td></tr>
<tr><td>15</td><td>15</td><td>15</td><td>15</td></tr>
</table>

Т1, Т2 ... Т11 – теми змістового модуля.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	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

10. Контрольні питання:

Питання, винесені на іспит чи залік.

1. Чому криптографічні алгоритми, що вимагають збереження в таємниці послідовності перетворення даних, не знаходять нині широкого застосування?
2. Яким має бути об'єм ключового простору для забезпечення криптографічної стійкості алгоритму?
3. Чи залежить криптографічна стійкість алгоритму від набору можливих символів ключа?
4. Що таке ключ?
5. Назвіть основні показники криптостійкості.
6. Охарактеризуйте заходи по захисту ключів.
7. Виходячи з чого визначається необхідність зміни ключів шифрування?
8. Які способи захисту від несанкціонованого копіювання програм Ви знаєте?
9. Охарактеризуйте спосіб захисту, що ґрунтується на використанні міток носія інформації.
10. Охарактеризуйте спосіб захисту, що ґрунтується на тимчасових характеристиках читання носія інформації.
11. Чи можна зберігати значення серійного номера пристрою, що перевіряється, не в тілі програми, а в окремому файлі?
12. Чи доцільно виділяти процедури, що здійснюють дії по захисту, в окремі динамічні бібліотеки?
13. Як коректно іменувати процедури, які здійснюють захисні механізми?
14. Які способи розповсюдження програмних продуктів ви знаєте?
15. Як організувати в тілі програми додаткові перевірки?

16. Що розуміють під незадокументованими точками входу в програму?
17. Що собою являє захист від несанкціонованого використання та копіювання?
18. Назвіть, будь ласка, групи систем захисту від несанкціонованого використання та копіювання.
19. Які існують методи захисту програмного забезпечення, шляхом прив’язки до параметрів комп’ютера?
20. Що відносять до шкідливого програмного забезпечення і як його класифікують?
21. Класифікуйте комп’ютерні віруси за середовищем їх існування та за способом зараження комп’ютерів.
22. Наведіть класифікацію вірусів за алгоритмами, які вони використовують при функціонуванні, та за своїми деструктивними можливостями.
23. Наведіть алгоритм роботи файлових вірусів.
24. В чому полягає принцип дії завантажувального вірусу?
25. Наведіть алгоритм роботи завантажувального вірусу: резидентного і нерезидентного.
26. Дайте загальну характеристику макро-вірусам, їх особливостям та розташуванню.
27. В чому особливості мережевих вірусів?
28. Охарактеризуйте стелс-віруси. Які різновиди цих вірусів ви знаєте?
29. Для чого існують і як функціонують конструктори вірусів та поліморфік-генератори?
30. Які існують методи і засоби для захисту від комп’ютерних вірусів?
31. За якими ознаками можна виявити факт зараження комп'ютерним вірусом?
32. Які заходи рекомендується вживати, щоб запобігти зараженню комп'ютерним вірусом?
33. Що таке антивірусна програма? Які типи антивірусів ви знаєте?
34. Охарактеризуйте різновиди антивірусних програм.
35. Які правила треба знати та виконувати, щоб не наражати свій комп'ютер на небезпеку зараження комп'ютерними вірусами?
36. Що треба робити, якщо ви виявили зараження комп'ютера вірусом?
37. Що таке антивірус?
38. Наведіть, будь ласка, класифікацію антивірусних програм.
39. Наведіть приклади антивірусів. Коротко охарактеризуйте їх.
40. Які основні функції антивірусів ви знаєте?
41. Чи можна заразити вірусом простий текстовий файл, що має розширення txt?
42. Які є методи контролю трафіку між локальної та зовнішньою мережею?
43. Яким чином може здійснюватися перехоплення трафіку?
44. Які є принципи дії брандмауера?
45. Що дозволяє виявити аналіз трафіку, який пройшов через сніффер?
46. За допомогою яких засобів можна знизити погрозу сніффингу пакетів?

47. Поняття інформаційної безпеки. Основні складові.
48. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
49. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: p = 7, q = 11, e= 43. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.
50. Основні визначення та класифікація загроз.
51. Екранування, аналіз захищеності.
52. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: p = 7, q = 11, e= 37. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.
53. Стандарти та специфікації в області інформаційної безпеки.
54. Адміністративний рівень інформаційної безпеки.
55. Управління ризиками в інформаційній безпеці.
56. Процедурний рівень інформаційної безпеки.
57. Основні поняття програмно-технічного рівня інформаційної безпеки.
58. Ідентифікація та автентифікація. Управління доступом.
59. Протоколювання та аудит, шифрування, контроль цілісності.

11. Рекомендована література:

Базова

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6
2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
3. Столлингс В. Криптография и защитасетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательскийдом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.
4. Сенів М.М., Яковина В.С. Безпека програм та даних / М.М. Сенів, В.С. Яковина. – Львів: Львівська політехніка, 2015. – 256 с.
5. Козіна Г.Л. Криптопротоколи: схеми цифрового підпису / Г.Л. Козіна, М.А. Молдовян, Г.В. Неласа. – Запоріжжя: ЗНТУ, 2014. – 158 с.
6. 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.

Допоміжна

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. Хорошко В. А. Методы и средствазашитыинформации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Інформаційні ресурси

9. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека програм та даних" https://pns.hneu.edu.ua/enrol/index.php?id=4941.