МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ІВАНА ФРАНКА

Кафедра безпеки інформації та бізнес-комунікацій

"ЗАТВЕРДЖУЮ"

В. о. завідувача кафедри безпеки
інформації та бізнес-комунікацій
д.е.н., проф.Хмелярчук М. І.
_____
"30" серпня 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ІНФОРМАЦІЙНА БЕЗПЕКА

рівень вищої освіти	*перший* *перший (бакалаврський) / другий (магістерський)*
галузь знань	*05 Соціальні та поведінкові науки* *шифр і назва*
спеціальність **освітня програма** **спеціалізація**	*051 Економіка* *код і назва* *Економічна кібернетика та бізнес-аналітика* *назва* _____ *назва*
статус дисципліни	*вибіркова* *обов'язкова / вибіркова /*
факультет	*Економічний*

2022-2023 навчальний рік

Робоча програма дисципліни «Інформаційна безпека» для студентів спеціальності 051 Економіка.

Розробник: кандидат економічних наук, доцент, доцент кафедри безпеки інформації та бізнес-комунікацій
Циганчук Роман Олегович

Робочу програму схвалено на засіданні кафедри кафедри безпеки інформації та бізнес-комунікацій

Протокол від “30” серпня 2022 року № 1

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, освітній рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма здобуття освіти</td><td>заочна форма здобуття освіти</td></tr>
<tr><td rowspan="2">Кількість кредитів – 6</td><td>Галузь знань
05 Соціальні та поведінкові науки</td><td colspan="2" rowspan="2">за вибором</td></tr>
<tr><td></td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">Освітній рівень:
бакалаврський</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 2</td><td>4-й</td><td>-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання
_____
(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td></td><td>1-й</td><td>-й</td></tr>
<tr><td>Загальна кількість годин – 180</td><td rowspan="15">Спеціальність:
051 Економіка</td><td colspan="2">Лекції</td></tr>
<tr><td rowspan="14">Тижневих годин для денної форми здобуття освіти :
аудиторних – 4
самостійної роботи студента – 7,25</td><td>32 год.</td><td>год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>32 год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>116 год.</td><td>год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">год.</td></tr>
<tr><td colspan="2">Вид контролю:
(екзамен/залік)</td></tr>
<tr><td>залік</td><td></td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми здобуття освіти – 35,6% і 64,4 відповідно.

2. Мета та завдання навчальної дисципліни

Мета вивчення дисципліни: формування термінологічного фундаменту; навчання студентів правильно проводити аналіз загроз інформаційній безпеці; ознайомити з основними методами, принципами, алгоритмами захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданням дисципліни є ознайомлення студентів з основними методами обробки інформації, існуючими технологіями захисту інформації і практичними навичками з їх створення, впровадження і супроводження.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- теорію побудови систем захисту інформації;
- криптографічні методи обробки інформації;
- технології зберігання інформації;
- методи захисту від комп'ютерних вірусів;
- основи технології контролю мережевого трафіку.

вміти:

- виконувати розрахунки контрольних сум, надмірних циклічних кодів;
- проводити перетворення інформації з метою передачі за каналами зв'язку;
- аналізувати захищеність комп'ютерних мереж від зовнішніх загроз, користуватися спеціальною та довідковою літературою;
- розробляти захищені вузли з обробки інформації.

Результатами навчання за навчальною дисципліною «Інформаційна безпека» є:

Таблиця 1

Код	Заплановані результати навчання за навчальною дисципліною
РНД 1	демонструє знання сучасних загроз безпеці інформаційних систем та технічних методів і засобів захисту інформації;
РНД 2	розуміє роль та сутність процесів криптографічних методів захисту інформації;
РНД 3	володіє знаннями аналізу програмних методів і засобів захисту інформації;
РНД 4	самостійно аналізує можливості несанкціонованого здобуття інформації потенційними порушниками;
РНД 5	демонструє знання організаційно-правового забезпечення захисту інформації правил макетування та верстки у веб-дизайні;
РНД 6	аналізує вплив шкідливих програм на безпеку інформаційних систем;
РНД 7	досліджує стійкість секретних криптографічних систем;
РНД 8	володіє вмінням організовувати та виконувати практичні дії працівників відділу безпеки інформації відповідно до посадових інструкцій.

3. Програма навчальної дисципліни

4.

ЗМІСТОВИЙ МОДУЛЬ 1. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ.

ТЕМА 1. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ.

Поняття безпеки інформаційних систем. Системні принципи забезпечення безпеки. Політика безпеки. Аналіз ризиків. План захисту. Класифікація інформації. Класифікація загроз. Ненавмисні загрози. Навмисні загрози.

ТЕМА 2. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ.

Канали несанкціонованого витоку інформації. Класифікація каналів витоку інформації: радіо, акустичний, електричний, візуально-оптичний, матеріально-речовий. Лінії зв'язку. Канали витоку інформації при експлуатації ЕОМ.

ТЕМА 3. ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕНАВМИСНИХ ЗАГРОЗ.

Класифікація методів захисту інформації від ненавмисних загроз. Способи контролю правильності передавання даних. Код з перевіркою на парність. Код Хемінга, циклічні коди, код Вітербі. Ефективне стискання інформації. Алгоритм Шеннона-Фано, алгоритм Хафмана, LZW-стискання.

ТЕМА 4. ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ.

Принципи захисту інформації від несанкціонованого доступу (локального доступу, віддаленого доступу). Методи ідентифікації та автентифікації користувачів. Біометрична автентифікація.

ТЕМА 5. ТЕХНІЧНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ.

Класифікація технічних засобів захисту. Технічні засоби захисту території та об'єктів. Захист ліній зв'язку. Екранування приміщень. Захист від навмисної силової дії.

ЗМІСТОВИЙ МОДУЛЬ 2. КРИПТОГРАФІЧНІ ТА БАЗОВІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ.

ТЕМА 6. ТЕОРІЯ ОПТИМАЛЬНИХ СИСТЕМ.

Класифікація шифрів. Стійкість шифрів. Основні типи криптоаналітичних атак. Симетрична криптографія. Блочне шифрування. Мережа Фейстеля. Стандарт шифрування DES. Стандарт шифрування ГОСТ. Асиметрична криптографія. Хешування. Система шифрування RSA, система шифрування Ель Гамаля. Електронний цифровий підпис. Сучасні алгоритми ЕЦП.

Протоколи узгодження ключів. Цифровий конверт. Цифрова дата. Дворівнева сертифікація відкритих ключів. Інфраструктура відкритих ключів. Апаратні шифратори. Шифропроцесори. Принципи розробки програмного інтерфейсу. Ключові схеми. Електронний замок. Варіанти технічної реалізації.

ТЕМА 7. ПРОГРАМНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.

Загальна характеристика та класифікація зловмисних програм. Засоби мережевих атак та шпигунства. Антивірусні програми. Сканери безпеки. Програмні засоби захисту Windows. Програми внутрішнього захисту звичайна та ускладнена процедура впізнавання користувача методи особливо надійного впізнавання методи впізнавання інформаційної системи та її елементів користувачем, регулювання використання ресурсів. Програми захисту програм: захист програм від копіювання. Програми ядра системи безпеки: програми контролю.

ТЕМА 8. ЗАХИСТ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.

Міжмережеві екрани. Конфігурування вбудованого міжмережевого екрану. Активізація функції виявлення атак. Віртуальні приватні мережі, принципи їх функціонування. Організація приватних мереж та створення логічних дисків з крипто захистом. Протоколи, що забезпечують безпеку в Інтернеті IPSec, SSL, TLS, S/MIME, SET.

ТЕМА 9. СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Поняття інцидента інформаційної безпеки. Методи та засоби управління інцидентами інформаційної безпеки. Автоматизація управління інцидентами інформаційної безпеки за допомогою netForensics.

ТЕМА 10. ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ.

Основні міжнародні стандарти інформаційної безпеки ISO/IEC 27001:2005, ISO/IEC 27002:2005, Оранжева книга. ГОСТ 28147-89. Вимоги до безпеки інформаційних систем, введені в Україні. Організаційні заходи по захисту інформації.

4. Структура навчальної дисципліни

Назва теми	Кількість годин									
	Денна форма					Заочна (дистанційна) форма				
	Лекції	Практичні (семінарські) заняття	Лабораторні (контактні) заняття	Індивідуальні заняття	Самостійна робота студента	Лекції	Практичні (семінарські) заняття	Індивідуальні заняття	Заняття в дистанційному режимі	Самостійна робота
ЗМІСТОВИЙ МОДУЛЬ І. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ. (теми 1-5)										
Тема 1. Основи безпеки інформаційних систем	4	4	-	-	10	-	-	-	-	-
Тема 2 . Канали витоку інформації	3	3	-	-	10	-	-	-	-	-
Тема 3. Захист інформації від ненавмисних загроз	3	3	-	-	10	-	-	-	-	-
Тема 4. Захист від несанкціонованого доступу	3	3	-	-	10	-	-	-	-	-
Тема 5. Технічні методи та засоби захисту інформації в інформаційних системах	4	4			13	-	-	-	-	-
ЗМІСТОВИЙ МОДУЛЬ 2. КРИПТОГРАФІЧНІ ТА БАЗОВІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ. (теми 6-10)										
Тема 6. Теорія оптимальних систем	3	3	-	1	10	-	-	-	-	-
Тема 7. Програмні методи та засоби захисту інформації	3	3	-	1	10	-	-	-	-	-
Тема 8. Захист інформації в розподілених інформаційних системах	3	3	-	-	13	-	-	-	-	-
Тема 9. Система управління інцидентами інформаційної безпеки	3	3	-	-	15	-	-	-	-	-
Тема 10. Організаційно-правове забезпечення захисту інформації	3	3	-	-	13	-	-	-	-	-
Підсумковий контроль: залік										
Разом:	годин	180								
	кредитів	6								

5. Теми семінарських занять

Семінарські заняття не передбачені навчальним планом.

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин

1	Тема 1. Основи безпеки інформаційних систем	4
2	Тема 2 . Канали витоку інформації	3
3	Тема 3. Захист інформації від ненавмисних загроз	3
4	Тема 4. Захист від несанкціонованого доступу	3
5	Тема 5. Технічні методи та засоби захисту інформації в інформаційних системах	4
6	Тема 6. Теорія оптимальних систем	3
7	Тема 7. Програмні методи та засоби захисту інформації	3
8	Тема 8. Захист інформації в розподілених інформаційних системах	3
9	Тема 9. Система управління інцидентами інформаційної безпеки	3
10	Тема 10. Організаційно-правове забезпечення захисту інформації	3

7. Теми лабораторних занять

Лабораторні заняття не передбачені навчальним планом.

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи безпеки інформаційних систем	10
2	Тема 2 . Канали витоку інформації	10
3	Тема 3. Захист інформації від ненавмисних загроз	10
4	Тема 4. Захист від несанкціонованого доступу	10
5	Тема 5. Технічні методи та засоби захисту інформації в інформаційних системах	13
6	Тема 6. Теорія оптимальних систем	10
7	Тема 7. Програмні методи та засоби захисту інформації	10
8	Тема 8. Захист інформації в розподілених інформаційних системах	13
9	Тема 9. Система управління інцидентами інформаційної безпеки	15
10	Тема 10. Організаційно-правове забезпечення захисту інформації	13

9. Індивідуальні завдання

Індивідуальні завдання не передбачені навчальним планом.

10. Методи навчання

Вивчення дисципліни «Інформаційна безпека» спрямоване на формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах і лініях телекомунікаційного зв’язку в умовах широкого використання сучасних інформаційних технологій.

Міждисциплінарні зв`язки: дисципліна «Інформаційна безпека» ґрунтується на знаннях, отриманих при вивченні таких курсів як «Економічний аналіз», «Цифрова економіка», «Вища математика», «Теорія ймовірностей», «Інформаційні технології (рівень А)» та інших курсів.

Дисципліна «Інформаційна безпека» складається з двох змістових модулів:

1. Основи безпеки інформаційних систем.

2. Криптографічні та базові методи та засоби захисту інформації в інформаційних системах.

Методи навчання:

Інтерактивні лекції (проблемні лекції, лекції-дискусії, лекції-демонстрації з використанням мультимедійного обладнання);

Практичні заняття (навчальні дискусії, мозковий штурм, розв'язок ситуаційних вправ (кейсів));

Самостійне навчання (індивідуальна робота, робота в групах).

Лекції надають здобувачам основний теоретичний матеріал, що є основою для самостійного навчання, а також сприяють розвитку у здобувачів вищої освіти здатності до узагальнення та критичного мислення через участь в дискусіях. Лекції доповнюються практичними заняттями, що надають здобувачам вищої освіти можливість застосовувати теоретичні знання на реальних прикладах. Практичні заняття сконструйовані з застосуванням методів практико-орієнтованого навчання, і передбачають розв'язок здобувачами вищої освіти кейсів на основі можливих реальних ситуацій та виконання необхідних розрахунків. Самостійне навчання сприяє підготовці до лекцій, практичних занять, а також роботи індивідуально та в невеликих групах для підготовки презентацій, що будуть представлені іншим групам, та для виконання індивідуальних та групових ситуаційних вправ на практичних заняттях, участі в них тощо.

11. Методи контролю

Критерії оцінювання

1. Критерієм успішного проходження здобувачем освіти оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.
2. Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати його в мінімальну позитивну оцінку числової (рейтингової) шкали, що використовується.

Засоби оцінювання

Засобами оцінювання результатів навчання можуть бути:

– стандартизовані тести;

– аналітичні звіти, реферати, есе;
– розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; розрахункові роботи;
– інші види індивідуальних та групових завдань.

Форми поточного та підсумкового контролю

1. Форма підсумкового контролю за навчальною дисципліною «Інформаційна безпека» - залік.
2. Форми поточного контролю під час навчальних занять: усні відповіді. Розв'язування задач та практичних завдань, письмове опитування у формі самостійних та контрольних робіт, написання економічних есе.
3. Розподіл балів які може накопичувати здобувач при вивченні дисципліни «Інформаційна безпека», наведено в таблиці

Таблиця 2

Форми контролю результатів навчання студентів за навчальною дисципліною «Інформаційна безпека» та їх оцінювання

Форми контролю	Максимальна кількість балів
	Денна форма навчання
Поточний контроль:	
Усні відповіді, розв'язування задач та практичних завдань	10 х 5 = 50 балів
Письмові опитування	до 30 балів
Підсумкова контрольна робота	20 балів
Всього за результатами поточного контролю:	100
Всього	100

В таблиці 2 зазначено система оцінювання результатів виконання студентами всіх видів робіт, що передбачені робочою програмою навчальної дисципліни «Інформаційна безпека».

12. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота										Сума
Змістовий модуль 1					Змістовий модуль 2					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	100
10	10	10	10	10	10	10	10	10	10	

Т1, Т2 ... Т10 – теми змістових модулів.

Шкала оцінювання: національна та ЄКТС

Оцінка ЄКТС	Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
A	90 – 100	відмінно	зараховано
B	81-89	добре	
C	71-80		
D	61-70	задовільно	
E	51-60		
FX	21-50	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
F	0-20	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

13. Методичне забезпечення

1. Робоча програма навчальної дисципліни.

2. Силабус навчальної дисципліни.

14. Рекомендована література

Базова

1. Закон України «Про електронний цифровий підпис»;
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
3. Закон України «Про інформацію»;
4. Закон України "Про захист інформації в автоматизованих системах"
5. Вимоги до системи управління інформаційною безпекою. СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010.
6. Положення про контроль за функціонуванням системи технічного захисту інформації. Затверджено наказом ДСТСЗІ СБ України від 22.12.99.№ 61.
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
9. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.
11. В. Фурашев. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки // "Інформація і право". – № 1(4)/2012. – С. 46 – 55.
12. В. Фурашев Сутність та визначення понять "інформаційна безпека" і "безпека інформації" // "Правова інформатика". – № 2(34)/2012. – С. 51 – 59.
13. Фурашев В.М. Ключові аспекти проекту Закону України "Про безпеку інформації" // "Віче". – 2012. – № 6/2012(315). – С. 29 – 30.
14. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.
15. National Military Strategy for Cyberspace Operations. – Режим доступу : //www.dod. gov/pubs/foi/ojcs/07-F-2105doc1.pdf
16. Glossary and Acronyms (Archived) / European Commission. – (Accessed 03 Nov 2009). – Режим доступу : //www.ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c
17. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. – Режим доступу : //www.official-document/cm76/7642/7642.pdf
18. The French White Paper on defence and national security. – Режим доступу : //www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf
19. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України / Г.В. Новицький. – К. : Інтертехнологія, 2008. – 496 с.
20. Хлевицький В.Б. Інформаційна безпека як одна із складових національної безпеки України / В.Б. Хлевицький // Євроатлантикінформ. – 2006. – № 1(7). – С. 70 – 72.
21. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности / І.Л. Бачило // Информатика и вычислительная техника. – 1992. – №2. – С. 22 – 30.
22. Брижко В. До питання застосування у правотворчості понять "інформація" та "дані" / В. Брижко // Правова інформатика. – 2005. – № 4 (8). – С. 31 – 37.
23. Калюжний Р. Проблеми та перспективи правового забезпечення безпеки інформації з обмеженим доступом, що не становить державної таємниці / Р. Калюжний, Д. Прокоф'єва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник / НТУУ "КПІ", Міністерство освіти і науки України, Департамент

спеціальних телекомунікаційних систем та захисту інформації СБ України. – К., 2000. – С. 27 – 31.
24. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б.А. Кормич. – Одеса : Юридична література, 2003. – 472 с.
25. Марущак А.І. Правомірні засоби доступу громадян до інформації : науково-практичний посібник / А.І. Марущак. – Біла Церква : Вид-во "Буква", 2006. – 432 с.
26. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія / В.Б. Толубко. – К. : НАОУ, 2003. – 315 с.
27. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.
28. Колодюк О.В. Національні стратегії інформаційного суспільства: необхідність, переваги та стан щодо запровадження в Україні / О.В. Колодюк – Режим доступу : http: //www.isu.org.ua/viewarticale/publications/117?new_lang=u.