ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАТИКИ ТА ФІЗИКО-МАТЕМАТИЧНИХ ДИСЦИПЛІН

«ЗАТВЕРДЖУЮ»
Декан факультету
інформаційних технологій
_____ /Повхан І.Ф./
«1» _____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**126 Інформаційні системи та технології**
Освітня програма	**Управління ІТ проектами**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2022

Робоча програма навчальної дисципліни «**Безпека інформаційних систем**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **126 Інформаційні системи та технології** освітньої програми **«Управління ІТ проектами».**

Розробник: Лях І. М. доц., к.т.н., доцент кафедри інформатики та фізико-математичних дисциплін

Робочу програму розглянуто та затверджено на засіданні **кафедри інформатики та фізико-математичних дисциплін**
протокол №12 від «20» червня 2022 р.
Завідувач кафедри _____ Василь КУТ

Схвалено науково-методичною комісією факультету інформаційних технологій
протокол №14 від «21» червня 2022 р.
Т.в.о. Голови науково-методичної комісії _____Ігор ПОВХАН

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th>Найменування показників</th><th colspan="2">Розподіл годин за навчальним планом</th></tr>
<tr><td></td><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 150</td><td>1 - й</td><td>1 - й</td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 5,5</td><td>1 – й</td><td>1 - й</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>32</td><td>10</td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>20</td><td>6</td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:
екзамен</td><td>-</td><td>-</td></tr>
<tr><td rowspan="6">Форма підсумкового контролю:
усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>98</td><td>134</td></tr>
<tr><td colspan="2">Індивідуальна робота:</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Безпека інформаційних систем»** є формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанкціонованому доступу на прикладі послуг безпеки в інформаційних системах, грамотного застосування механізмів захисту інформації на основі сучасних процедур криптосистем для забезпечення доступності, цілісності, конфіденційності, автентичності транзакцій та даних.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ІНТ. Здатність розв’язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій.

ФК 1. Здатність розробляти та застосувати ІСТ, необхідні для розв’язання стратегічних і поточних задач.

ФК 6. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна **«Безпека інформаційних систем»** не потребує попереднього вивчення компонентів освітньої програми.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Управління ІТ проектами»**, вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	**Шифр ПРН**
Приймати ефективні рішення з проблем розвитку інформаційної інфраструктури, створення і застосування ІСТ.	ПРН 3
Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.	ПРН 10

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Безпека інформаційних систем**»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Знати та розуміти принципи безпеки інформаційних систем; різні технологічні рішення, що використовуються для забезпечення безпеки інформаційних систем; мати навички прийняття ефективних рішень щодо безпеки інформаційних систем.	ПРН 3
Знати та вміти виявляти загрози, які можуть впливати на інформаційні системи; застосовувати різноманітні методи і технології захисту інформаційних систем; основні принципи та законодавство, пов'язані із захистом інформації.	ПРН 10

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- виступи на практичних заняттях;
- реферати;
- презентації;
- модульні контрольні роботи;
- екзамен.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: усне опитування, оцінювання виконання практичних завдань, написання самостійних робіт.

Форма модульного контролю: письмова контрольна робота.

Форма підсумкового семестрового контролю: усний екзамен.

Особливості використання засобів діагностики та контролю за умов дистанційного навчання

В умовах використання формату онлайн-навчання (дистанційного навчання) із застосуванням корпоративної мережі Google Meet названі засоби, методи і форми визначаються за домовленістю зі студентським колективом і, в залежності від зручного виду взаємодії, застосовуються з допомогою існуючих функцій групових чатів та відео-конференцій.

Для ефективного засвоєння тематики є можливість демонстрації необхідних матеріалів на робочому столі комп’ютерного технічного засобу під час занять.

Зокрема, у разі потреби, під час онлайн-заняття можна надати доступ до свого екрану, щоб показати презентації або іншу тематичну інформацію на робочому столі.

Планування лекційних і практичних (семінарських) занять, модульних контрольних робіт, а також підсумкова перевірка знань у формі екзамену (заліку) здійснюється заздалегідь за допомогою прив’язки до гугл-календаря.

Синхронізація запланованих заходів виконується автоматично на всіх зручних для їх проведення пристроях.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота					**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	70	**100**
6	6	6	6	6		

Т1, Т2… – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота					**Модульна контрольна робота**	**Сума**
Т6	Т7	Т8	Т9	Т10	70	**100**
6	6	6	6	6		

Т6, Т7… – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	5	20	5	20
Презентація	1	5	1	5
Реферат	1	5	1	5
Модульна контрольна робота	1	70	1	70
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

МК1 та МК2 складається з випадкових 7 описових питань теоретичного курсу. Максимальна кількість балів за кожне питання – 10 балів. Максимальна оцінка за модульний контроль – 100 балів. Якщо студент не був присутнім на модульному контролі, або бажає перездати - він має право його здати згідно розроблених процедур в Положенні про організацію освітнього процесу в ДВНЗ «Ужгородський національний університет».

Критерії оцінювання підсумкового семестрового контролю

До складання екзамену допускаються здобувачі вищої освіти, які мають підсумковий доекзаменаційний рейтинговий бал не менше 35.

Здобувач вищої освіти, доекзаменаційний рейтинговий бал якого складає від 0 до 34 балів, зобов'язаний покращити його до початку екзамену під час чергування викладачів на кафедрі у строки, визначені викладачем дисципліни та погоджені деканатом факультету. В протилежному випадку, здобувач не допускається до екзамену, і у нього виникає академічна заборгованість.

Екзамен з навчальної дисципліни здобувач вищої освіти може не складати, якщо він успішно пройшов усі модульні контролі та його влаштовує підсумкова доекзаменаційна рейтингова оцінка за навчальний рік. Здобувачі вищої освіти, рейтинговий бал яких становить від 35 до 59, екзамен складають обов'язково.

Здобувач освіти може підвищити на екзамені рейтинговий бал, при цьому, за результатами складання екзамену оцінка не може бути менша за доекзаменаційний рейтинговий бал.

Екзамен проводиться в усній формі. На екзамен виноситься навчальний матеріал семестру. Екзаменаційний білет складається з теоретичних питань. Оцінювання результатів навчання на екзамені здійснюється за 100-бальною шкалою. Оцінка за екзамен вноситься у відомість обліку успішності.

Переведення даних 100-бальної шкали оцінювання у оцінки занаціональною шкалою та шкалою ЄКТС

Сума балів	**Оцінка ЄКТС**	**Оцінка за національною шкалою**	
		екзамен, диф. залік	**залік**
90 -100	A	відмінно	зараховано
82 - 89	B	добре	
74 - 81	C		
64 - 73	D	задовільно	
60 - 63	E		
35 - 59	F X	незадовільно	не зараховано
0 - 34	F		

Оцінка відмінно (A) виставляється, коли студент дає абсолютно правильні відповіді на теоретичні питання з викладенням оригінальних висновків, отриманих на основі програмного, додаткового матеріалу та нормативних документів. При виконанні практичного завдання студентзастосовує системні знання навчального матеріалу, передбачені навчальною програмою.

Оцінка добре (B) виставляється студенту, який повністю розкривтеоретичні питання на основі програмного та додаткового матеріалу. При виконанні практичних завдань студент застосовує узагальнені знання навчального матеріалу, передбачені навчальною програмою.

Оцінка добре (C) виставляється студенту, який повністю розкривтеоретичні питання, а програмний матеріал викладено у відповідності до вимог. Практичні завдання виконані в цілому правильно, але мають місце окремі неточності.

Оцінка задовільно (D) виставляється, коли студент розкрив теоретичні питання, проте при викладенні програмного матеріалу допущені окремі помилки. При виконанні практичних завдань студент припускається помилок, за рахунок недостатнього розуміння програмного матеріалу.

Оцінка задовільно (E) виставляється, коли студент неповністю розкрив теоретичні питання, відповідь містить суттєві помилки. При виконанні практичних завдань студент припускається значних помилок, а виконання завдань викликає значні труднощі у студента.

Оцінка незадовільно (FX) виставляється студенту, який не розкрив теоретичні питання і не може виконати практичні завдання. Як правило такий студент виявляє здатність до викладення думки лише на елементарному рівні.

Оцінка незадовільно (F) виставляється студенту, який не виконав навчальну програму або якийсь серйозний елемент її складової, має фрагментарні знання, які не дозволяють розкрити теоретичні питання і виконати практичні завдання. Такий студент не може викласти свою думку навіть на елементарному рівні. За результатами контролю знань студентів, дозволяється виставлення екзаменаційної оцінки (без підсумкового екзамену) – «відмінно», «добре», та «задовільно». Студент має право підвищити оцінку, складаючи екзамен.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Тема 1. Захист інформації в каналах зв’язку.

Тема 2. Засоби несанкціонованого доступу до інформації.

Тема 3. Виявлення несанкціонованих засобів доступу до інформації.

Тема 4. Методи боротьби ВОЛЗ.

Тема 5. Інформаційна безпека в мережах коміркового зв’язку.

Тема 6. Захист від несанкціонованого доступу мережі GSM.

Тема 7. Захист від прослуховування.

Тема 8. Конфіденційність локалізації абонента.

Модуль 2

Тема 9. Види комп’ютерних мереж та їх основи функціонування.

Тема 10. Інциденти інформаційної безпеки.

Тема 11. Принципи організації безпеки комп’ютерних мереж.

Тема 12. Методи та засоби забезпечення вимог політики безпеки.

Тема 13. Види атак на інформаційні та програмно-технічні ресурси.

Тема 14. Виявлення атак на ресурси комп’ютерної мережі.

Тема 15. Захист приватної мережі від зовнішнього втручання.

Тема 16. Особливості забезпечення безпеки корпоративних мереж.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Форма навчання: денна						Форма навчання: заочна					
	Усього	у тому числі					Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
Модуль 1												
Тема 1. Захист інформації в каналах зв'язку		2				7		1				8
Тема 2. Засоби несанкціонованого доступу до інформації		2	2			6		1	1			8
Тема 3. Виявлення несанкціонованих засобів доступу до інформації		2	2			6						8
Тема 4. Методи боротьби ВОЛЗ		2				6		1				8
Тема 5. Інформаційна безпека в мережах коміркового зв'язку		2	2			6			1			8
Тема 6. Захист від несанкціонованого доступу мережі GSM		2	2			6		1				9
Тема 7. Захист від прослуховування		2	2			6			1			9
Тема 8. Конфіденційність локалізації абонента		2				6		1				9
Модульна контрольна робота		16	10			49		5	3			67
Разом за модуль		16	10			49		5	3			67
Модуль 2												
Тема 9. Види комп'ютерних мереж та їх основи функціонування		2				7		1				8
Тема 10. Інциденти інформаційної безпеки		2				6						8
Тема 11. Принципи організації безпеки комп'ютерних мереж		2	2			6		1	1			8
Тема 12. Методи та засоби забезпечення вимог політики безпеки		2	2			6		1	1			8
Тема 13. Види атак на інформаційні та програмно-технічні ресурси		2	2			6						8

Тема 14. Виявлення атак на ресурси комп'ютерної мережі		2	2			6		1				9
Тема 15. Захист приватної мережі від зовнішнього втручання		2	2			6		1	1			9
Тема 16. Особливості забезпечення безпеки корпоративних мереж		2				6						9
Модульна контрольна робота		16	10			49		5	3			67
Разом за модуль		16	10			49		5	3			67
Разом за семестр		**32**	**20**			**98**		**10**	**6**			**134**

6.3. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Засоби несанкціонованого доступу до інформації	2	1
2	Виявлення несанкціонованих засобів доступу до інформації	2	
3	Інформаційна безпека в мережах коміркового зв'язку	2	1
4	Захист від несанкціонованого доступу мережі GSM	2	
5	Захист від прослуховування	2	1
6	Принципи організації безпеки комп'ютерних мереж	2	1
7	Методи та засоби забезпечення вимог політики безпеки	2	1
8	Види атак на інформаційні та програмно-технічні ресурси	2	
9	Виявлення атак на ресурси комп'ютерної мережі	2	
10	Захист приватної мережі від зовнішнього втручання	2	1
	Разом	**20**	**6**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Захист інформації в каналах зв'язку	7	8
2	Засоби несанкціонованого доступу до інформації	6	8
3	Виявлення несанкціонованих засобів доступу до інформації	6	8
4	Методи боротьби ВОЛЗ	6	8
5	Інформаційна безпека в мережах коміркового зв'язку	6	8
6	Захист від несанкціонованого доступу мережі GSM	6	9
7	Захист від прослуховування	6	9
8	Конфіденційність локалізації абонента	6	9
9	Види комп'ютерних мереж та їх основи функціонування	7	8
10	Інциденти інформаційної безпеки	6	8
11	Принципи організації безпеки комп'ютерних мереж	6	8
12	Методи та засоби забезпечення вимог політики безпеки	6	8
13	Види атак на інформаційні та програмно-технічні ресурси	6	8
14	Виявлення атак на ресурси комп'ютерної мережі	6	9
15	Захист приватної мережі від зовнішнього втручання	6	9
16	Особливості забезпечення безпеки корпоративних мереж	6	9
	Разом	**98**	**134**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: мультимедійний проектор.

Обладнання: персональні комп'ютери, ноутбуки.

Програмне забезпечення: Microsoft Office, сервіс Google Meet, дистанційна платформа Moodle.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи: навч. посіб./ І. В. Горбатий, А. П. Бондарєв. - Львів: Видавництво Львівської політехніки, 2016. - 336 с.

2. Грищук Р. В. Основи кібернетичної безпеки: монографія/ Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, - Житомир: ЖНАЕ, 2016. - 636 с.

Допоміжна література

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К. : ДУТ, 2015. - 288 с.

Інформаційні ресурси в мережі Інтернет

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» https://zakon.rada.gov.ua/laws/show/3475-15#Text
2. Закон України «Про інформацію» https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
4. Закон України «Про основні засади забезпечення кібербезпеки України» https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Постанова КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

6. Постанова КМУ від 16 грудня 2020 р. № 1358 «Деякі питання функціонування Національної телекомунікаційної мережі» https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text

7. Наказ Адміністрації Держспецзв’язку від 20.09.2021 № 576 «Про затвердження Вимог щодо рівня якості послуг рухомого (мобільного) зв’язку» https://zakon.rada.gov.ua/laws/show/z1298-21#Text

Результати перегляду

робочої програми навчальної дисципліни

Робоча програма перезатверджена на 2023 / 2024 н.р. без змін; зі змінами (Додаток __).

(потрібне підкреслити)

протокол № 12 від «23» червня 2023 р. Завідувач кафедри ________ Василь КУТ

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток __).

(потрібне підкреслити)

протокол № ___ від «____» ________ 20___ р. Завідувач кафедри ________ ___________

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток __).

(потрібне підкреслити)

протокол № ___ від «____» ________ 20___ р. Завідувач кафедри ________ ___________

(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток __).

(потрібне підкреслити)

протокол № ___ від «____» ________ 20___ р. Завідувач кафедри ________ ___________

(підпис) (Прізвище ініціали)