ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ

«ЗАТВЕРДЖУЮ»
Декан факультету
інформаційних технологій
_____ /Повхан І.Ф./
«30» _____2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОГРАМНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Рівень вищої освіти	**перший (бакалаврський)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**121 Інженерія програмного забезпечення**
Освітня програма	**Інженерія програмного забезпечення**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2023

Робоча програма навчальної дисципліни **«Програмні технології захисту інформації»** для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **121 Інженерія програмного забезпечення** освітньої програми **«Інженерія програмного забезпечення».**

Розробник: Поліщук В. В. доц., д.т.н., професор кафедри програмного забезпечення систем

Робочу програму розглянуто та затверджено на засіданні **кафедри програмного забезпечення систем**

протокол №12 від «19» червня 2023 р.

Завідувач кафедри _____ Юрій БІЛАК

Схвалено науково-методичною комісією факультету інформаційних технологій

протокол №9 від «30» червня 2023 р.

Т.в.о. Голови науково-методичної комісії _____ Ігор ПОВХАН

Робоча програма перезатверджена на 20 24 / 20 25 н.р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № 11 від «15» 05 20 24 р.

Завідувач кафедри _____ Білан Ю.М.
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20 25 / 20 26 н.р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № 13 від «12» 05 20 25 р.

Завідувач кафедри _____ Білан Ю.М.
(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)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4,5</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 135</td><td>4 - й</td><td>4 - 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 – 4
самостійної роботи студента– 6</td><td>7- й</td><td>7 - й</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>28</td><td>10</td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td rowspan="2">Види підсумкового контролю: екзамен</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>24</td><td>4</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>83</td><td>121</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета вивчення навчальної дисципліни **«Програмні технології захисту інформації»** полягає в: освоєнні та розумінні програмних інструментів та методологій, які використовуються для захисту інформації в сучасному цифровому середовищі; аналіз загроз інформаційної безпеки, основними методам, принципам, алгоритмам захисту інформації в комп’ютерних та інформаційних системах, з урахуванням сучасних тенденцій розвитку інформаційної безпеки та кіберзахисту.

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

ІК Здатність розв’язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій.

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.

ФК 1. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

ФК 4. Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.

ФК 6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

ФК11. Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовою вивчення навчальної дисципліни **«Програмні технології захисту інформації»** є опанування такої навчальної дисципліни (НД) освітньої програми (ОП):

ОК 19 Об’єктно-орієнтоване програмування

ОК 21 Технологія програмування та створення програмних продуктів

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Інженерія програмного забезпечення»**, вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПР):

Програмні результати навчання	**Шифр ПР**
Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.	ПР 02
Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.	ПР 04
Знати і застосовувати відповідні математичні поняття,	ПР 05

методи доменного, системного і об’єктно орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.	
Знати та вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.	ПР 09
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.	ПР 21

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Програмні технології захисту інформації»**:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Усвідомлювати відповідальність за якість та безпеку програмного забезпечення, а також за впровадження етичних принципів у свою професійну діяльність; здатні аналізувати етичні дилеми, які можуть виникнути у процесі розробки та використання програмного забезпечення, та приймати обґрунтовані рішення на основі принципів професійної етики.	ПР 02
Розуміти важливість використання стандартів і документів для забезпечення якості та безпеки програмного забезпечення; застосовувати професійні стандарти та нормативно-правові документи при проектуванні, розробці та тестуванні програмного забезпечення.	ПР 04
Знати математичні методи та моделі для розробки програмного забезпечення, що використовується для захисту інформації від несанкціонованого доступу, зловживання та	ПР 05

втрати даних; знати важливість математичного моделювання при розробці програмного забезпечення і його вплив на якість та ефективність роботи програм.	
Вміти формулювати вимоги до програмного забезпечення з урахуванням потреб користувачів та інших зацікавлених сторін; знання різні методи та засоби збору вимог до програмного забезпечення для захисту інформації.	ПР 09
Знати різні засоби забезпечення інформаційної безпеки та цілісності даних, визначати вразливості та ризики; вміти аналізувати потреби в забезпеченні інформаційної безпеки та цілісності даних для конструювання програмних систем; знати вибирати відповідні засоби забезпечення інформаційної безпеки та цілісності даних залежно від конкретних вимог та потреб; знати кваліфікованого застосування засобів забезпечення інформаційної безпеки для забезпечення безпеки та цілісності програмних систем.	ПР 21

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:

- виконання та захист лабораторних робіт;
- реферати;
- модульні контрольні роботи;
- екзамен.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: виконання та захист лабораторних робіт.

Форма модульного контролю: письмове/тестове оцінювання.

Форма підсумкового семестрового контролю: усний екзамен.

Особливості застосування неформальної освіти

У сфері неформального навчання, реалізуються наступні види індивідуальних занять: сертифікатні програми, тренінги, короткотермінові курси, літні школи тощо під керівництвом тренерів, репетиторів та інших фахівців.

До онлайн-платформ, результати яких визнаються в межах дисципліни належать Udemy, Prometheus, Coursera, EdX, Udacity. Як альтернатива класичному заліку/екзамену, отримані результати навчання можуть бути зараховані у повному обсязі або частково, здобувачам освіти у їх формальному навчанні. Тобто студенти мають можливість отримати оцінку підсумкового контролю із окремих дисциплін на основі отриманих результатів на вище визначених онлайн-платформах.

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 лабораторних занять, модульних контрольних робіт, а також підсумкова перевірка знань у формі екзамену 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	Т6	50	**100**
8	8	8	8	9	9		

Т1, Т2… − теми

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

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т7	Т8	Т9	Т10	Т11	Т12	50	**100**
8	8	9	8	9	8		

Т7, Т8… − 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)
Лабораторні роботи	5	40	5	40
Реферат	1	10	1	10
Модульна контрольна робота	1	50	1	50
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

МК1 та МК2 складається з випадкових 20 тестових питань теоретичного курсу. Максимальна кількість балів за кожне питання – 3,5 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 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 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 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.

Також здобувач може отримати підсумкову оцінку в рамках неформальної освіти. У випадку, якщо години/кредити ЄКТС в отриманому студентом сертифікаті про успішне завершення відповідного курсу повністю співпадають з годинами/кредитами ЄКТС визначеними для даної дисципліни чи перевищують їх, то результати зараховуються у повному обсязі, у іншому випадку можливе тільки часткове зарахування.

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

<table>
<tr><th rowspan="2">Сума балів</th><th rowspan="2">Оцінка ЄКТС</th><th colspan="2">Оцінка за національною шкалою</th></tr>
<tr><th>екзамен, диф. залік</th><th>залік</th></tr>
<tr><td>90 -100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82 - 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74 - 81</td><td>C</td></tr>
<tr><td>64 - 73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60 - 63</td><td>E</td></tr>
<tr><td>35 - 59</td><td>FX</td><td rowspan="2">незадовільно</td><td rowspan="2">не зараховано</td></tr>
<tr><td>0 - 34</td><td>F</td></tr>
</table>

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 студент застосовує системні знання навчального матеріалу, передбачені навчальною програмою.

Оцінка добре (B) виставляється студенту, який повністю розкрив теоретичні 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 розкрив теоретичні 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

екзаменаційну оцінки (без підсумкового заліку) – «відмінно», «добре», та «задовільно». Студент має право підвищити оцінку, складаючи екзамен.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Тема 1. Вступ. Проблеми теорії захисту інформації.

Тема 2. Характеристика загроз безпеки інформації

Тема 3. Несанкціонований доступ. Порушники безпеки

Тема 4. Шляхи забезпечення безпеки інформації: Концепція захисту інформації; Стратегія та архітектура захисту інформації; Види забезпечення безпеки інформації.

Тема 5. Політика безпеки інформації: Етапи реалізації систем захисту.

Тема 6. Моделі політики безпеки: Дискреційна політика безпеки; Мандатна політика безпеки; Рольова політика безпеки; Монітор безпеки.

Модуль 2

Тема 7. Криптографічні методи захисту інформації: Основні положення та визначення; Характеристика алгоритмів шифрування.

Тема 8. Методи захисту інформації в операційних системах.

Тема 9. Аналіз безпеки ПЗ та руйнуюче ПЗ.

Тема 10. Методи аналізу безпеки ПЗ.

Тема 11. Поняття про гешувальні алгоритми, їх призначення, вимоги до них.

Тема 12. Поняття про цифровий підпис, вимоги до нього. Основні положення керування ключами.

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. Вступ. Проблеми теорії захисту інформації.	11	2		2		7	11	1				10
Тема 2. Характеристика загроз безпеки інформації	11	2		2		7	11	1				10
Тема 3. Несанкціонований доступ. Порушники безпеки	11	2		2		7	11	1				10
Тема 4. Шляхи забезпечення безпеки інформації: Концепція захисту інфор-мації; Стратегія та архітектура захисту інформації; Види забезпечення безпеки ін-формації.	11	2		2		7	11			1		10
Тема 5. Політика безпеки інформації: Етапи реалізації систем захисту.	11	2		2		7	11	1				10
Тема 6. Моделі політики безпеки: Дискреційна політика безпеки; Мандатна політика безпеки; Рольова політика безпеки; Монітор безпеки.	13	4		2		7	12	1		1		10
Модульна контрольна робота	**68**	**14**		**12**		**42**	**67**	**5**		**2**		**60**
Разом за модуль	**68**	**14**		**12**		**42**	**67**	**5**		**2**		**60**
Модуль 2												
Тема 7. Криптографічні методи захисту інформації: Основні положення та визначення; Характеристика алгоритмів шифрування.	11	2		2		7	11	1				10
Тема 8. Методи захисту інформації в операційних системах.	12	4		2		6	12	1		1		10
Тема 9. Аналіз безпеки ПЗ та руйнуюче ПЗ.	11	2		2		7	11	1				10
Тема 10. Методи аналізу безпеки ПЗ.	11	2		2		7	11			1		10

Тема 11. Поняття про гешувальні алгоритми, їх призначення, вимоги до них.	11	2		2		7	12	1				11
Тема 12. Поняття про цифровий підпис, вимоги до нього. Основні положен-ня керування ключами.	11	2		2		7	11	1				10
Модульна контрольна робота	67	14		12		41	68	5		2		61
Разом за модуль	67	14		12		41	68	5		2		61
Разом за семестр	**135**	**28**		**24**		**83**	**135**	**10**		**4**		**121**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Вступ. Проблеми теорії захисту інформації.	2	
2	Характеристика загроз безпеки інформації	2	
3	Несанкціонований доступ. Порушники безпеки	2	
4	Шляхи забезпечення безпеки інформації: Концепція захисту інфор-мації; Стратегія та архітектура захисту інформації; Види забезпечення безпеки ін-формації.	2	1
5	Політика безпеки інформації: Етапи реалізації систем захисту.	2	
6	Моделі політики безпеки: Дискреційна політика безпеки; Мандатна політика безпеки; Рольова політика безпеки; Монітор безпеки.	2	1
7	Криптографічні методи захисту інформації: Основні положення та визначення; Характеристика алгоритмів шифрування.	2	
8	Методи захисту інформації в операційних системах.	2	1
9	Аналіз безпеки ПЗ та руйнуюче ПЗ.	2	
10	Методи аналізу безпеки ПЗ.	2	1
11	Поняття про гешувальні алгоритми, їх призначення, вимоги до них.	2	
12	Поняття про цифровий підпис, вимоги до нього. Основні положен-ня керування ключами.	2	
	Разом	**24**	**4**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Вступ. Проблеми теорії захисту інформації.	7	10
2	Характеристика загроз безпеки інформації	7	10
3	Несанкціонований доступ. Порушники безпеки	7	10
4	Шляхи забезпечення безпеки інформації: Концепція захисту інфор-мації; Стратегія та архітектура захисту інформації; Види забезпечення безпеки ін-формації.	7	10
5	Політика безпеки інформації: Етапи реалізації систем захисту.	7	10
6	Моделі політики безпеки: Дискреційна політика безпеки; Мандатна політика безпеки; Рольова політика безпеки; Монітор безпеки.	7	10
7	Криптографічні методи захисту інформації: Основні положення та визначення; Характеристика алгоритмів шифрування.	7	10
8	Методи захисту інформації в операційних системах.	6	10
9	Аналіз безпеки ПЗ та руйнуюче ПЗ.	7	10

10	Методи аналізу безпеки ПЗ.	7	10
11	Поняття про гешувальні алгоритми, їх призначення, вимоги до них.	7	11
12	Поняття про цифровий підпис, вимоги до нього. Основні положен-ня керування ключами.	7	10
	Разом	**83**	**121**

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. Методичні вказівки до лабораторних робіт: Програмні технології захисту інформації / [уклад.: В.В. Поліщук]. – Ужгород: УжНУ, 2023. – 31 с.
2. Бобало Ю. Я. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Сенів М. М., Яковина В. С. Безпека програм та даних. Навчальний посібник. Львів : Видавництво Львівської політехніки, 2015. 256 с.
4. Юдін О. К. Захист інформації в мережах передачі даних: підручник МОН України / О. К. Юдін, Г. Ф. Конахович, О. Г. Корченко. - К. :, 2009. - 714 с.

Допоміжна література

1. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

2. Березюк Б. М. Системи і мережі передавання даних: навч. посіб. / Б. М. Березюк. - Серія “Дистанційне навчання”. № 34. - Львів : Вид-во Національного університету “Львівська політехніка”, 2005. - 200 с.
3. 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. Про захист персональних даних [Електронний ресурс]: закон України № 2297-VI: [прийнятий Верховною Радою України 2010 р. : редакція від 27 жовтня 2022 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
2. Про інформацію [Електронний ресурс]: закон України № 2657-XII: [прийнятий Верховною Радою України 1992 р. : редакція від 21 березня 2023 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: закон України № 2163-VIII: [прийнятий Верховною Радою України 2017 р. : редакція від 17 серпня 2022 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про державну таємницю [Електронний ресурс]: закон України № 3855-XII: [прийнятий Верховною Радою України 1994 р. : редакція від 31 березня 2023 р.]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

Результати перегляду
робочої програми навчальної дисципліни

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)

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

протокол № ___ від «____» ________ 20___ р. Завідувач кафедри ________ ___________
(підпис) (Прізвище ініціали)