Рівненський державний гуманітарний університет

Кафедра інформаційних технологій та моделювання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ

Спеціальність **121 Інженерія програмного забезпечення**

Освітня програма **«Інженерія програмного забезпечення»**

Рівень вищої освіти **перший (бакалаврський)**

Факультет **математики та інформатики**

2024-2025 навчальний рік

Робоча програма навчальної дисципліни «Захист інформації» для здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності 121 Інженерія програмного забезпечення за освітньою програмою «Інженерія програмного забезпечення»

Мова навчання: українська

Розробники: Кіндрат П.В. кандидат юридичних наук, доцент кафедри Інформаційно-комунікаційних технологій та методики викладання інформатики

Робоча програма затверджена на засіданні кафедри інформаційних технологій та моделювання.

Протокол від 27 серпня 2024 року № 8.

Завідувач кафедри  Мороз І. П.

Робочу програму схвалено навчально-методичною комісією факультету математики та інформатики.

Протокол від 3 вересня 2024 року № 7.

Голова навчально-методичної комісії  Гнедко Н. М.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="20">Кількість кредитів: 4
Модулів: 2
Змістових модулів: 2
Індивідуальне науково-дослідне завдання: система безпечного обміну інформацією через публічну мережу
Загальна кількість годин: 120
Тижневих годин: аудиторних 3 самостійної роботи студента 6</td><td rowspan="20">Галузь знань:
12 Інформаційні технології
Спеціальність:
121 Інженерія програмного забезпечення
Освітня програма:
«Інженерія програмного забезпечення»
Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td><td>Обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td>4</td><td>4</td></tr>
<tr><td colspan="2">Семестр:</td></tr>
<tr><td>8</td><td>8</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні:</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота:</td></tr>
<tr><td>80</td><td>108</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Передумови для вивчення дисципліни: «Кросплатформне програмування», «Операційні системи».

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Захист інформації» відноситься до обов’язкових компонентів професійної підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю 121 Інженерія програмного забезпечення. Робоча програма навчальної дисципліни складена у відповідності до освітньо-професійної програми «Інженерія програмного забезпечення» підготовки бакалаврів за названою спеціальністю.

Освітній компонент вивчає відмінності та особливості налаштувань програмного і мережевого рівнів інформаційної безпеки; місце захисту інформації на різних етапах життєвого циклу програмного забезпечення. Він передбачає розвиток у студентів здатності до аналізу вразливостей інформаційних систем; побудови комплексного захисту інформаційних систем; розробляти як індивідуальні так і колективні проекти з захисту інформаційних систем. А також вироблення уміння застосовувати криптографічні засоби для підвищення захищеності інформації.

Метою викладання навчальної дисципліни «Захист інформації» є засвоєння здобувачами вищої освіти основних понять та категорій безпеки інформації та інформаційної безпеки, вивчення принципів побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів симетричної та асиметричної криптографії для забезпечення автентичності, цілісності та конфіденційності інформаційних систем.

Основними **завданнями** вивчення дисципліни «Захист інформації» є ознайомлення студентів з основними поняттями та положеннями захисту інформації, вивчення ними

основних методів збереження конфіденційності та цілісності інформації, а також методів підтримки її доступності.

Згідно з освітньо-професійною програмою навчальна дисципліна «Захист інформації» має забезпечити формування у здобувачів вищої освіти відповідних **компетентностей.**

Загальні компетентності

К02. Здатність застосовувати знання у практичних ситуаціях.

К06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К22. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті освоєння повного курсу навчальної дисципліни «Захист інформації» у здобувачів вищої освіти формуються глибокі, міцні і системні знання, які передбачають вільне володіння понятійним апаратом, розуміння основних задач предмету, його мети та завдання, а також здатність до практичного застосування цих знань при реалізації прикладних застосувань. Згідно з освітньо-професійною програмою мають бути досягнуті наступні **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.

Здобувачі вищої освіти мають

знати:

- основні складові інформаційної безпеки;
- критерії класифікації загроз інформаційній безпеці;
- типові загрози апаратного, програмного та мережевого рівнів;
- міжнародні та вітчизняні стандарти захисту інформації;
- класифікацію криптографічних систем;
- криптографічні програмні інтерфейси;
- типи криптоатак;

вміти:

- належним чином налаштовувати програмний і мережевий рівні інформаційної безпеки;
- здійснювати проектування безпеки апаратно-програмних комплексів як цілісного об’єкту;
- аргументовано імплементувати положення міжнародних та вітчизняних стандартів захисту інформації в розроблювані програмні продукти;
- визначати загрози інформаційній безпеці та здійснювати пошук і розробку рішень для усунення виявлених загроз;
- реалізовувати відомі алгоритми шифрування інформації;
- розробляти системи захисту від зчитування інформації з урахуванням та усвідомленням сильних та слабких сторін криптографічного захисту;
- створювати та верифікувати цифрові підписи електронних документів.

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. «Основи інформаційної безпеки та захисту інформації»

Тема 1. Поняття інформаційної безпеки та захисту інформації. Основні складові інформаційної безпеки. Доступність. Цілісність. Конфіденційність. Важливість і складність проблеми інформаційної безпеки. Загрози. Основні визначення і критерії класифікації загроз. Загрози доступності даних. Основні загрози цілісності даних. Загрози конфіденційності даних. Протидія загрозам.

Тема 2. Апаратні засоби захисту інформації. Шкідливі зовнішні фізичні фактори. Основи апаратного захисту. Апаратні засоби захисту. Класифікація технічних засобів зняття інформації. Спеціальні пристрої прослуховування. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Основні стаціонарні засоби захисту інформації. Пошукове устаткування.

Тема 3. Програмні засоби захисту інформації. Шкідливе програмне забезпечення. Комп'ютерні віруси. Класифікація комп'ютерних вірусів. Антивірусне програмне забезпечення. Проблеми безпеки програмного забезпечення. Помилки в програмному забезпеченні та «чорні ходи» у ньому. Невірне адміністрування. Основні методи захисту: від вірусів, від незадокументованих можливостей ПЗ (закладок), від несанкціонованого використання ПЗ, від дефектів ПЗ.

Тема 4. Захист інформації в комп'ютерних мережах. Проблеми безпеки мереж. Рівні безпеки мережевих систем. Джерела загроз у мережах. Види загроз і протидія їм. Атаки на мережеві системи. Атака на апаратуру. Атака на файловий сервер. Атака на пароль. Атака перехопленням і нав'язуванням пакета. Атаки на канал зв'язку. Проблеми безпеки web-застосувань. Захист комп'ютерних систем від несанкціонованого доступу. Міжмережеві екрани та монітори безпеки (системи виявлення атак).

Змістовий модуль 2. «Крипторграфія»

Тема 5. Криптографія. Основні поняття. Криптографія. Криптографічна система. Вимоги до криптографічних систем. Класифікація криптографічних систем.

Тема 6. Симетричні криптосистеми. Класифікація симетричних криптосистем. Шифри заміни. Шифри перестановки. Блочні шифри. Режими застосування блочних шифрів. Приклади симетричних криптосистем

Тема 7. Асиметричні криптосистеми. Однобічні функції. Функції-пастки. Шифри з відкритим та закритим ключами. Приклади асиметричних криптосистем. Шифр Рівеста-Шаміра-Алдемана (RSA). Функції хешування та їх використання. Електронний цифровий підпис та його використання

Тема 8. Криптографічні програмні інтерфейси та їх використання. Microsoft CryptoAPI. Структура CryptoAPI. Криптопровайдер. Криптографічні ключі. Сесійні ключі. Пари відкритий/закритий ключ. Робота з ключами. Збереження ключів. Контейнери. Шифрування і дешифрування даних. Цифровий підпис. Створення та перевірка цифрового підпису.

Тема 9. Елементи криптоаналізу. Криптоаналіз. Елементи криптоаналізу. Криптоатака. Типи криптоатак. Криптоаналіз найпростіших шифрів. Метод повного перебору.

5. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин											
	денна форма навчання						заочна форма навчання					
	усього	у тому числі				інд	усього	у тому числі				інд
		лек	пр	лаб	с.р.			лек	пр	лаб	с.р.	
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1. «Основи інформаційної безпеки та захисту інформації»												

Тема 1. Поняття інформаційної безпеки та захисту інформації	12	4			8		48	2		2	44	
Тема 2. Апаратні засоби захисту інформації	12	2		2	8							
Тема 3. Програмні засоби захисту інформації	12	2		2	8							
Тема 4. Захист інформації в комп'ютерних мережах	12	2		2	8							
Разом за змістовим модулем 1	**48**	**10**	**-**	**6**	**32**	**-**	**48**	**2**	**-**	**2**	**44**	**-**
Змістовий модуль 2. «Крипторграфія»												
Тема 5. Криптографія. Основні поняття	12	2		2	8		72	4		4	64	
Тема 6. Симетричні криптосистеми	14	2		2	10							
Тема 7. Асиметричні криптосистеми	16	2		4	10							
Тема 8. Криптографічні програмні інтерфейси та їх використання	16	2		4	10							
Тема 9. Елементи криптоаналізу	14	2		2	10							
Разом за змістовим модулем 2	**72**	**10**	**-**	**14**	**48**	**-**	**72**	**4**	**-**	**4**	**64**	**-**
Модуль 2												
ІНДЗ												
Усього годин	**120**	**20**	**-**	**20**	**80**	**-**	**120**	**6**	**-**	**6**	**108**	**-**

6. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

Не передбачено навчальним планом

7. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Не передбачено навчальним планом

8. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з.п.	Назва теми	Кількість годин
1.	Протидія засобам дистанційного зчитування інформації	2
2.	Протидія шкідливому програмному забезпеченню	2
3.	Проблеми безпеки мережевих-застосувань	2
4.	Найпростіші алгоритми шифрування даних	2
5.	Симетричні криптосистеми. Стандарт DES	2
6.	Асиметричні криптосистеми. Стандарт RSA	2
7.	Цифровий підпис. Стандарт DSA	2
8.	Криптографічні програмні інтерфейси компільованих мов програмування	2
9.	Криптографічні програмні інтерфейси інтерпритованих мов програмування	2
10.	Криптоаналіз найпростіших криптосистем	2
	Разом	**20**

9. САМОСТІЙНА РОБОТА

№ з.п.	Назва теми	Кількість годин
1.	Сутність та зміст понять інформаційної безпеки та безпеки інформації.	6
2.	Апаратні загрози безпеці інформації	6
3.	Програмні загрози безпеці інформації	6
4.	Вразливості програмних систем	7
5.	Вразливості мережевих систем	7
6.	Криптографічні методи захисту, їх переваги та недоліки.	8
7.	Блочні шифри	8
8.	Стандарти симетричного шифрування	8
9.	Стандарти асиметричного шифрування	8
10.	Криптографічні програмні інтерфейси та їх використання	8
11.	Аналіз методів криптоаналізу відомих шифрів.	8
	Разом	**80**

10. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

В якості індивідуального завдання студентам пропонується виконання творчого завдання «Організація безпечного обміну інформацією через публічну мережу». Кожен студент пропонує та реалізовує свою концепцію організації захисту інформації.

11. МЕТОДИ НАВЧАННЯ

МН1 – словесний метод (лекція, дискусія, обговорення досліджуваного явища чи процесу, аналіз проблемних ситуацій);
МН2 – практичний метод (лабораторні заняття);
МН3 – наочний метод (ілюстрації, демонстрації);
МН5 – інтерактивний метод (із застосуванням аудіо, відео, новітніх інформаційних технологій та комп'ютерних засобів навчання);
МН6 – самостійна робота (самостійний аналіз, проектування та програмна реалізація індивідуальних завдань);
МН7 – індивідуальна науково-дослідна робота здобувачів вищої освіти (виконання індивідуальних розрахункових робіт).

12. МЕТОДИ ОЦІНЮВАННЯ

МО1 – екзамен;
МО2 – усне або письмове опитування під час лабораторних занять;
МО4 – тестування;
МО7 – презентація та обговорення результатів виконаних індивідуальних розрахункових робіт;
МО9 – захист лабораторних робіт.

13. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

- перевірка (усна, письмова) рівня засвоєння теоретичного матеріалу за навчальними темами;
- перевірка рівня сформованості практичних умінь і навичок студентів під час

проведення практичних і лабораторних занять;

- перевірка виконання студентами завдань, запропонованих для домашнього опрацювання;
- перевірка рівня засвоєння студентами навчальних тем, призначених для самостійного опрацювання;
- усний або письмовий експрес-контроль;
- колоквіум;
- контрольна робота;
- перевірка рефератів;
- підсумкове комплексне тестування за модулем;
- формою підсумкового контролю є екзамен як спосіб комплексної перевірки та диференційованого оцінювання якості засвоєння студентами навчального матеріалу з курсу та набуття професійно зорієнтованих компетентностей.

Види та методи навчання і оцінювання

Код ЗК, СК	Назва компетентності	Код ПРН	Назва програмного результату навчання	Методи навчання	Методи оцінювання
К02	Здатність застосовувати знання у практичних ситуаціях.	ПР07	Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9
		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.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9
К06	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	ПР07	Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9
		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.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9
К18	Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки)	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.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9
К22	Здатність накопичувати, обробляти та	ПР07	Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9

	систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.		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.	МН1, МН2, МН3, МН5, МН6, МН7	МО1, МО2, МО4, МО7, МО9

14. КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результат освітньої діяльності здобувача вищої освіти оцінюється згідно Положення про оцінювання знань і умінь здобувачів вищої освіти РДГУ за такими критеріями оцінювання та рівнями компетентності:

Суми балів за 100-бальною шкалою	**Оцінка в ЄКТС**	**Значення оцінки ЄКТС**	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка за національною шкалою**
90-100	A	відмінно	здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить і опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні здібності	високий (творчий)	відмінно
82-89	B	добре	здобувач вищої освіти вільно володіє теоретичним матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	достатній (конструктивно-варіативний)	добре
74-81	C	добре	здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача, загалом самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, з-поміж яких є суттєві, добирати аргументи для підтвердження думок	достатній (конструктивно-варіативний)	добре
64-73	D	задовільно	здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння	середній (репродуктивний)	задовільно

			основних положень, за допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, з-поміж яких є значна кількість суттєвих		
60-63	E	задовільно	здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	середній (репродуктивний)	задовільно
35-59	FX	незадовільно з можливістю повторного складання семестрового контролю	здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	низький (рецептивно-продуктивний)	незадовільно
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об'єктів	низький (рецептивно-продуктивний	незадовільно

Підсумкова (загальна) оцінка з навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювальні форми навчальної діяльності: поточне і підсумкове оцінювання рівня засвоєння теоретичного та практичного матеріалу під час аудиторних занять і самостійної роботи; оцінка (бали) за виконання лабораторних завдань; оцінка (бали) за індивідуальну науково-дослідну роботу; оцінка (бали) за участь у наукових конференціях, олімпіадах, підготовку наукових публікацій, рефератів тощо.

15. РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ ЗДОБУВАЧІ ВИЩОЇ ОСВІТИ

В університеті діє накопичувальна кредитно-трансферна система оцінювання програмних результатів навчання студентів, що реалізується в ході виконання і захисту лабораторних робіт, виконання ІНДЗ та модульного контролю, для яких визначено мінімальну кількість балів, яку слід набрати для формування рейтингового балу студента та виставлення його у залікову книжку і відомість успішності студентів з відповідними оцінками за національною та європейською кредитно-трансферною системами (ЄКТС).

Розподіл балів за видами освітньої діяльності

П'ятибальна система оцінок	3,	4,	5
Робота на лекційних заняттях			1
Захист лабораторних робіт	1,	2,	3
Модульний контроль	3,	4,	5
ІНДЗ	4,	7,	10
Екзамен			40

Поточне тестування та самостійна робота									ІНДЗ	Екзамен	**Сума**
Змістовий модуль 1				Змістовий модуль 2							
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9			
2	4	4	4	4	4	7	7	4			
Модульний контроль – 5				Модульний контроль – 5							
19				**31**					**10**	**40**	**100**

Т1, Т2, ..., Т9 – теми змістових модулів

16. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Самостійна робота студентів над теоретичним та практичним матеріалом навчальної дисципліни здійснюється в таких формах:

- вивчення теоретичного матеріалу, що викладений на лекційних заняттях та призначеного для самостійного опрацювання;
- індивідуальне виконання навчальних завдань, розв'язування алгоритмічних задач та завдань по розробці алгоритмів та програмуванню.

В якості навчально-методичного забезпечення самостійної роботи студентів використовується базова та додаткова література з дисципліни, Інтернет-ресурси, матеріал лекцій, методичні рекомендації для виконання лабораторних робіт.

17. ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ПІДСУМКОВОГО КОНТРОЛЮ

1. Основні складові інформаційної безпеки. Доступність. Цілісність. Конфіденційність.
2. Важливість і складність проблеми інформаційної безпеки.
3. Загрози. Основні визначення і критерії класифікації загроз.
4. Загрози доступності даних. Основні загрози цілісності даних. Загрози конфіденційності даних. Протидія загрозам.
5. Законодавчий та адміністративний рівні інформаційної безпеки.
6. Процедурний рівень інформаційної безпеки. Керування персоналом. Фізичний захист. Підтримка працездатності.
7. Реагування на порушення режиму безпеки. Планування відновлювальних робіт.
8. Програмно-технічний рівень інформаційної безпеки. Ідентифікація та аутентифікація.
9. Керування доступом. Протоколювання і аудит. Шифрування.
10. Контроль цілісності. Екранування. Аналіз захищеності. Тунелювання.
11. Забезпечення безвідмовності та безпечного відновлення.
12. Шкідливі зовнішні фізичні фактори. Шкідливе програмне забезпечення.
13. Комп'ютерні віруси. Класифікація комп'ютерних вірусів.
14. Антивірусне програмне забезпечення. Проблеми безпеки програмного забезпечення.
15. Помилки в програмному забезпеченні та «чорні ходи» у ньому. Невірне адміністрування.
16. Можливість фізичного доступу зловмисника до ЕОМ.
17. Основні методи захисту від вірусів, від незадокументованих можливостей ПЗ (закладок), від несанкціонованого використання ПЗ, від дефектів ПЗ.
18. Проблеми безпеки мереж. Рівні безпеки мережевих систем.
19. Джерела загроз у мережах. Види загроз і протидія їм.
20. Атаки на мережеві системи. Атака на апаратуру.
21. Атака на файловий сервер. Атака на пароль. Атака перехопленням і нав'язуванням пакету атаки на канал зв'язку. Проблеми безпеки web-застосувань.
22. Захист комп'ютерних систем від несанкціонованого доступу.
23. Міжмережеві екрани та монітори безпеки (системи виявлення атак).
24. Апаратні засоби захисту.
25. Криптографія. Криптографічна система.
26. Вимоги до криптографічних систем. Класифікація криптографічних систем
27. Класифікація симетричних криптосистем. Шифри заміни. Шифри перестановки
28. Блочні шифри. Режими застосування блочних шрифтів.
29. Приклади симетричних крипто систем.
30. Однобічні функції. Функції-пастки.
31. Шифри з відкритим та закритим ключами.
32. Приклада асиметричних криптосистем.

33. Шифр RSA.
34. Шифр Ель-Гамаля.
35. Функції хешування та їх використання.
36. Електронний цифровий підпис та його використання.
37. Microsoft CryptoAPI. Структура CryptoAPI. Криптопровайдер.
38. Криптографічні ключі. Сесійні ключі. Пари відкритий/закритий ключ. Робота з ключами. Збереження ключів. Контейнери.
39. Шифрування і петифрування даних. Цифровий підпис. Створення та перевірка цифрового підпису.
40. Криптоаналіз. Елементи криптоаналізу.
41. Криптоатака. Типи криптоатак. Криптоаналіз найпростіших шифрів. Метод лінійного перебору.

18. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Вишня В.Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки : Навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою : навч. посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
3. Інформаційна безпека / За ред. Ю.Я. Бобала та І.В. Горбатого. Львів : «Львівська політехніка», 2019. 540 с.
4. Інформаційна безпека : Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова. К. : Видавництво Ліра-К, 2021. 412 с.
5. Гапак О.М. Криптоаналіз. Криптографічні протоколи : Навч. посібник. Ужгород : видавництво ПП «АУТДОР-ШАРК», 2021р. 96 с.
6. Бем М.В., Городиський І.М. Стандарти захисту персональних даних в соціальній сфері. Львів: б.в., 2018. 110 с.
7. Тарнавський Ю.А. Технології захисту інформації : Підручник. К.: КПІ ім. Ігоря Сікорського, 2018. 162 с.

Допоміжна:

1. Nigel Cawthorne. Alan Turing: The Enigma Man. Acturus, 2019. 128 p.
2. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту : Навч. посібник. Львів : «Новий Світ-2000», 2020. 678 с.
3. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого; уклад.: С. А. Горбаченко, Н. І. Логінова. Одеса, 2020. 148 с.
4. Євсеєв С.П., Король О.Г. Кібербезпека: лабораторний практикум з основ криптографічного захисту. Львів : « Новий світ-2000», 2021. 241 с.
5. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.
6. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації : Навч. посібн. Одеса : Фенікс, 2015. 264 с.
7. Касперський І.П., Князєв С.О., Матяш О.І. та ін. Організаційно-правові основи захисту службової 0-64 інформації : Навч. посібник. Київ : Нац. акад. СБУ, 2017. 120 с.
8. Гуз А.М., Касперський І.П., Князєв С.О. та ін. Організація захисту інформації з обмеженим доступом : Навч. посібник. К. : Нац. акад., СБУ, 2018. 252 с.

19. ІНФОРМАЦІЙНІ (ІНТЕРНЕТ) РЕСУРСИ

- Institute of Electrical and Electronics Engineers [електронний ресурс] http://www.ieee.org
- ISO: Global standards for trusted goods and services [електронний ресурс] https://www.iso.org/home.html

- Дії криптографії [електронний ресурс] https://learn.microsoft.com/uk-ua/power-automate/desktop-flows/actions-reference/cryptography
- Методичні матеріали дисципліни [електронний ресурс]: https://drive.google.com/drive/folders/1n2jD_Q5qnsteRy-Xpesyov4vVMow34mA?usp=drive_link