НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра комп'ютерних та інформаційних технологій і систем

ЗАТВЕРДЖУЮ
Проректор із науково-педагогічної
та навчальної роботи
_____ А.М. Мартиненко
«30» 08 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист інформації»
(назва навчальної дисципліни)

підготовки **бакалавра**
(назва ступеня вищої освіти)
спеціальності **029 «Інформаційна, бібліотечна та архівна справа»**
(код і назва спеціальності)

Полтава
2024 рік

Робоча програма навчальної дисципліни «Захист інформації» для здобувачів вищої освіти спеціальності 029 «Інформаційна, бібліотечна та архівна справа».
Складена відповідно до освітньої програми підготовки першого (бакалаврськогоо) рівня вищої освіти «Інформаційна аналітика та PR-діяльність» 2024 року.

Розробник: Головко Г.В., к.т.н., доцент кафедри комп'ютерних та інформаційних технологій і систем

Погоджено:

Гарант освітньої програми _____ **Людмила ЧЕРЕДНИК**

Робочу програму затверджена на засіданні кафедри комп'ютерних та інформаційних технологій і систем
Протокол від 19.08. 2024 року № 1

Завідувач кафедри
комп'ютерних та інформаційних технологій і систем

_____ **Олена ДВІРНА**

«19» серпня 2024 року

Схвалено навчально-методичною комісією Навчально-наукового інституту інформаційних технологій та робототехніки
Протокол від «19» 08 2024 року № 1

Голова навчально-методичної комісії Навчально-наукового
інституту інформаційних технологій та робототехніки
_____ **Олександр ШЕФЕР**

«20» 08 2024 року

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, ступінь вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>форма навчання денна</td></tr>
<tr><td>Кількість кредитів – 6</td><td rowspan="2">Галузь знань
02 Культура і мистецтво</td><td rowspan="2">вибіркова</td></tr>
<tr><td>Загальна кількість годин – 180</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="6">Спеціальність
029 «Інформаційна, бібліотечна та архівна справа»</td><td>Рік підготовки:</td></tr>
<tr><td rowspan="5">2-й</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td></tr>
<tr><td>Семестр</td></tr>
<tr><td rowspan="5">3-й</td></tr>
<tr><td rowspan="11">Індивідуальне завдання – не передбачено</td><td rowspan="11">Ступінь вищої освіти

Бакалавр</td></tr>
<tr><td>Лекції</td></tr>
<tr><td>36 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>0 год..</td></tr>
<tr><td>Практичні</td></tr>
<tr><td>36 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>108 год.</td></tr>
<tr><td>Індивідуальна робота
0 год.</td></tr>
<tr><td>Вид контролю: диф. залік</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 72/108

2. Мета навчальної дисципліни

Навчальна дисципліна циклу вибіркової підготовки «Захист інформації» спрямована на опанування студентами теоретичних та практичних знань і навичок з методології аналізу причин порушення безпеки інформації, вибору політики безпеки та використовування сучасних методів закриття інформації.

3. Передумови для вивчення дисципліни

Навчальна дисципліна «Захист інформації» ґрунтується на таких дисциплінах: «Інформатика і комп'ютерна техніка», «Правові основи документно-інформаційної діяльності»

4. Очікувані результати навчання з дисципліни

Результати вивчення дисципліни «Захист інформації»:

Здатність застосовувати знання у практичних ситуаціях.

Навички використання інформаційних і і комунікативних технологій.

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

Здатність виявляти, ставити та вирішувати проблеми.

Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності.

Здатність здійснювати відбір, аналіз, оцінку,

систематизацію, моніторинг, організацію, зберігання, розповсюдження та надання в користування інформації та знань у будь-яких форматах.

Здатність використовувати методи систематизації, пошуку, збереження, класифікації інформації для різних типів контенту та носіїв..

5. Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом вивчення навчальної дисципліни.

Мінімальний порогів рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати в мінімальну позитивну оцінку числової (рейтингової) шкали.

Сума балів	**Значення ЄКТС**	**Оцінка**	**Критерій оцінювання**	**Рівень компетентності**

Сума балів	Значення ЄКТС	Оцінка	Критерій оцінювання	Рівень компетентності
90-100	**A**	**Відмінно**	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Власні пропозиції Здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін.	**Високий**, що повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82-89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною..	**Достатній**, що забезпечує Здобувачу самостійне вирішення основних практичних задач.
74-81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для вирішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.
64-73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.

Сума балів	Значення ЄКТС	Оцінка	Критерій оцінювання	Рівень компетентності
60-63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використанням основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній,** що є мінімально допустимим у всіх складових навчальної дисципліни
35-59	**FX**	**Незадовільно** з можливістю повторного складання екзамену/ заліку	фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних і лабораторних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький**, не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.
0-34	**F**	**Незадовільно** з обов'язковим повторним вивченням дисципліни	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний**, Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є: захист лабораторних робіт, тестування, диференційований залік.

7. Програма навчальної дисципліни

Змістовий модуль 1. Поняття інформаційної безпеки і її місце в системі національної безпеки.

Тема 1. Види і джерела погроз ІБ. Система нормативно-правових актів, що

регламентують забезпечення ІБ. Види інформації. Основні поняття захисту інформації(об'єкти, суб'єкти, канали витоку, НСД, рівні доступу). Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ.Поняття політики забезпечення ІБ. Структура, задачі служби Інформаційної безпеки

Практичне заняття 1-2

Тема 2. Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки.. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки.

Практичне заняття 3-4

Тема 3. Внутрішні механізми розмежування доступу (маркери доступу і дескриптори захисту), структура і призначення, участь маркерів доступу і дескрипторів захисту в процедурі одержання суб'єктів доступу до об'єктів ОС Механізми аудита і протоколювання в ОС Windows, класи зареєстрованих подій, керування аудитом (включення, відключення аудита визначених подій), аудит доступу до об'єктів і реєстру, журнали аудита, правила звертання з журналами аудита. Права ФС NTFS, призначення прав, керування правами, визначення діючих прав, перевірка прав при звертанні до об'єкта ФС.

Практичне заняття 5-6

Змістовий модуль 2. Організація захисту інформації

Тема 4. Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Особливості організації захисту від різних видів шкідливого програмно забезпечення.. Файлово-серверна і клієнт-серверна архітектури: опис, переваги і недоліки системи з колективним використанням файлів,системи з архітектурою клієнт-сервер: організація, переваги і недоліки.

Практичне заняття 7-8

Тема 5. **Кібератаки та кібертероризм: поняття і визначення.** Кібератаки та кібертероризм, поняття і визначення. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу

Практичне заняття 9-10

Тема 6 Криптологія, основні поняття, історія винекнення.

Практичне заняття 11-12

Тема 7 Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Класична шифри. Криптографічні і стеганографічні методи захисту інформації..

Практичне заняття 13-14

Тема 8 Симетричні шифри. Види симетричних шифрів. Математичні алгоритми. Стандарти симетричних шифрів

Практичне заняття 15-18

8. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
Змістовий модуль 1. Поняття інформаційної безпеки і її місце в системі національної безпеки.						
Тема 1 Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ. Види інформації. Основні поняття захисту інформації(об'єкти, суб'єкти, канали витоку, НСД, рівні доступу). Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ.Поняття політики забезпечення ІБ. Структура, задачі служби Інформаційної безпеки.	18	4	4	-	-	10
Тема 2. Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки.	18	4	4	-	-	10
Тема 3. Внутрішні механізми розмежування доступу (маркери доступу і дескриптори захисту), структура і призначення, участь маркерів доступу і дескрипторів захисту в процедурі одержання суб'єктів доступу до об'єктів ОС Механізми аудита і протоколювання в ОС Windows, класи зареєстрованих подій, керування аудитом (включення, відключення аудита визначених подій), аудит доступу до об'єктів і реєстру, журнали аудита, правила звертання з журналами аудита. Права ФС NTFS, призначення прав, керування правами, визначення діючих прав, перевірка прав при звертанні до об'єкта ФС.	20	4	4	0	-	12
Змістовий модуль 2. Організація захисту інформації .						
Тема 4. Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Особливості організації захисту від різних видів шкідливого програмно забезпечення.. Файлово-серверна і клієнт-серверна архітектури: опис, переваги і недоліки системи з колективним використанням файлів,системи з архітектурою клієнт-сервер: організація, переваги і недоліки.	20	4	4	-	-	12
Тема 5 Кібератаки та кібертероризм: поняття і визначення**.** Кібератаки та кібертероризм, поняття і визначення. Особливості реалізації атак і заходи з послаблення їхнього	22	4	4	-		14

деструктивного впливу						
Тема 6 Криптологія, основні поняття, історія винекнення	22	4	4	0		14
Тема 7. Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Класична шифри. Криптографічні і стеганографічні методи захисту інформації.	26	6	4	0		16
Тема 8 Симетричні шифри. Види симетричних шифрів. Математичні алгоритми. Стандарти симетричних шифрів	34	6	8	0		20
Разом за змістовим модулем 1	**180**	**36**	**36**		**-**	**108**
Усього годин	**180**	**36**	**36**		**-**	**108**

9. Перелік питань для семінарських занять

№ з/п	Перелік питань	Кількість годин
	Семінарські заняття не передбачені	-

10. Перелік питань для практичних занять

№ заняття	Перелік питань	Кількість годин
1-2	Основні поняття захисту інформації. Система нормативно-правових актів, що регламентують забезпечення ІБ. Види інформації	4
3-4	Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ**.** Види інформації. Основні поняття захисту інформації(об'єкти, суб'єкти, канали витоку, НСД, рівні доступу).	4
5-6	Структура, задачі служби інформаційної безпеки. Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ. Поняття політики забезпечення ІБ. Поняття погрози ІБ.	4
7-8	Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Особливості організації захисту від різних видів шкідливого програмно забезпечення	4
9-10	Основа побудови систем мандатного розмежування доступу. Модель Белла-Лападули як основа побудови систем мандатного розмежування доступу. Основні положення моделі.	4
11-12	Комп’ютерні віруси і боротьба з ними	4
13-14	Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем	4

№ заняття	Перелік питань	Кількість годин
15-18	Криптографічні методи захисту інформації Комплексний захист інформації	8
	Разом	**36**

11. Перелік питань для лабораторних занять

№ з/п	Перелік питань	Кількість Годин
	Лабораторних занять не передбачено	-

12. Самостійна робота

Мета самостійної роботи студента полягає у тому, щоб навчитися користуватися бібліотечними фондами і каталогами, працювати з літературними джерелами та Інтернет-ресурсами, складати конспекти, аналізувати матеріал, порівнювати різні наукові концепції та робити висновки.

Види самостійної роботи студента: опрацювання лекційного матеріалу; підготовка до лабораторних занять; опрацювання тем курсу, які виносяться на самостійне вивчення; підготовка до поточного контролю; відвідування консультацій (згідно з затвердженим графіком консультацій кафедри комп'ютерних та інформаційних технологій і систем); підготовка до складання диференційованого заліку.

Питання
для самостійного вивчення студентами

№ з/п	Перелік питань	Кількість годин
1	Законодавчі акти України в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю.	12
2	Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ. Поняття політики забезпечення ІБ	12
3	Збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС	12
4	Облікові записи користувачів і груп, збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження	12

№ з/п	Перелік питань	Кількість годин
	інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС	
5	Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози.	14
6	Кібератаки та кібертероризм	16
7	Криптографічні алгоритми для захисту інформації.	14
8	Комплексний захист інформації.	16
	Разом	**108**

13. Індивідуальні завдання

Не передбачено планом.

14. Методи навчання

Під час проведення лекцій та практичних занять використовуються такі вербальні методи як лекція, дискусія, співбесіда. До числа наочних методів, які застосовуються при викладанні навчальної дисципліни, належать: ілюстрація, демонстрація, робота в групах, участь у дискусіях та обговореннях, презентації результатів виконаних завдань та досліджень, метод мозкового штурму.

15. Методи контролю

Поточний контроль успішності засвоєннями студентами навчального матеріалу може здійснюватися шляхом опитування й оцінювання знань студентів під час лабораторних занять, оцінювання виконання студентами самостійної роботи та індивідуальних завдань, проведення і перевірки письмових контрольних робіт, тестування або в ході індивідуальних співбесід зі студентами під час консультацій. Вибір конкретних форм і методів поточного контролю знань студентів залежить від викладача і доводиться до їхнього відома на першому практичному занятті.

Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння студентом певної сукупності знань та вмінь, що формують відповідний модуль. Він реалізується шляхом проведення спеціальних контрольних заходів (у формі тестування чи написання студентами контрольних робіт), проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу студентів. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація).

Підсумковий контроль здійснюється у формі диференційованого заліку.

16. Розподіл балів, які отримують студенти

Схема нарахування балів для денної форми навчання з навчальної дисципліни «Захист інформації» за видами робіт

Види робіт/контролю	*Перелік тем*

	Тема 1	*Тема 2*	*Тема 3*	*Тема 4*	*Тема 5*		*Тема 6*		*Тема 7*			*Тема 8*	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Виконання лабораторних робіт	3	3	3	3	3	3	3	3	3	3	3	3	3
Тестування		1	1	1	1		1		1			1	
Самостійна робота (тестування)	1	1	1	1	1		1		1			1	
Разом за темою	4	5	5	5	10		10		13			10	
Диференційований залік	**30**												
Всього за результатами вивчення навчальної дисципліни	**100**												

*В таблиці вказана максимальна кількість балів, які можна набрати за видами робіт

Шкала та критерії оцінювання виконання лабораторної роботи

Бали	Критерії оцінювання
3	Завдання виконано повністю, всі вимоги лабораторної роботи дотримані. Відповідь правильна, логічно структурована та оформлена згідно з вимогами. Код (якщо передбачено) працює без помилок і містить необхідні коментарі.
2,5-2,9	Завдання виконано повністю, але містить незначні неточності або помилки, які не впливають на загальну правильність виконання. Код працює, проте може мати незначні стилістичні або логічні недоліки.
2,1-2,5	Завдання виконано на 75% і більше, але є неточності або пропущені важливі аспекти. Код містить дрібні помилки, які легко виправити.
1,1-2,1	Завдання виконано більш ніж на 50%, проте є значні недоліки або помилки. Код містить помилки, що заважають його коректному виконанню.
0,5-1	Завдання виконано менш ніж на 50%, відповідь містить суттєві помилки або пропуски. Код (якщо передбачено) не працює або містить критичні помилки.
0-0,4	Завдання не виконано або виконано менш ніж на 15%, відповідь відсутня або нерозбірлива. Код (якщо передбачено) відсутній або повністю некоректний.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання диференційованого заліку

Завдання	Бали	Критерії оцінювання
Тестування	0-30	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×30=30), правильність відповідей перевіряється відповідно до ключа тестів.

Оцінювання тестування:

- кожна правильна відповідь оцінюється у фіксовану кількість балів (0,1×10=1);
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання виконання завдань самостійної роботи (тестування)

Завдання	Бали	Критерії оцінювання
Тестування	0-1	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×0,1=1), правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання виконання контрольної роботи

Бали	Критерії оцінювання
38-31	Відповідь надана у письмовій формі, повна (не менше 90% потрібної інформації) та правильна.
25-28	Відповідь надана у письмовій формі, повна (не менше 80% потрібної інформації) з незначними неточностями
20-24	Відповідь надана у письмовій формі, достатньо повна (не менше 75% потрібної інформації) правильна.
	Відповідь надана у письмовій формі, достатньо повна (не менше 75% потрібної інформації) з незначними неточностями.
10-19	Відповідь надана у письмовій формі, неповна (не менше 60% потрібної інформації) з несуттєвими помилками.
	Відповідь надана у письмовій формі, коротка (менше 30% потрібної інформації) із помилками.
0-9	Відповідь надана у письмовій формі, коротка (менше 15% потрібної інформації) із суттєвими помилками
	Відповідь відсутня.

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ECTS	Оцінка за національною шкалою для екзамену, курсової роботи
90-100	**A** - відмінно	5-відмінно
82-89	**B**-дуже добре	4-добре
74-81	**C**-добре	
64-73	**D**-задовільно	3-задовільно
60-63	**E**-достатньо	
35-59	**FX**-незадовільно з можливістю повторного складання	2-незадовільно
0-34	**F**-незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них до 70 балів студент може отримати впродовж семестру, решта 70 балів припадає на підсумковий контроль.

1. Поточний контроль:

Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином (розподіл орієнтовний):

- робота на лабораторних заняттях (відповіді на практичних заняттях, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних лабораторних занять) – до 70 балів).

Присутність на лекціях і лабораторних заняттях не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів, при тривалій відсутності студента на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

Студент, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (не менше 30 балів поточної успішності), допускається до підсумкового контролю з дисципліни.

2. Підсумковий контроль: Підсумковим контролем є диференційований залік. Він здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті імені Юрія Кондратюка».

17. Методичне забезпечення

1. Методичні рекомендації до виконання лабораторних занять та самостійної роботи студентів з дисципліни «Захист інформації» спеціальності 029 «Інформаційна, бібліотечна та архівна справа» для студентів всіх форм навчання / Укладач: Головко Г.В. Полтава: Національний університет імені Юрія Кондратюка, 2024. 47 с.

18. Рекомендована література

Базова

1. Kubernetes and Docker - An Enterprise Guide: Effectively containerize applications, integrate Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.

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

3. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.

4. Головко Г.В. Лабораторний практикум з дисципліни «Захист інформації» для спеціальності «Інформаційна, бібліотечна та архівна справа» для студентів всіх форм навчання Національний університет «Полтавська політехніка імені Юрія Кондратюка». – Полтава, 2022. 59 с.

5. Задірака В.К., Олексюк О. С. Комп'ютерна криптологія : підручник / Терноп. акад. нар. госп-ва, НАН України, Ін-т кібернетики ім. В. М. Глушкова. Київ : Вид-во «Збруч», 2002. 504 с.

6. Василюк, В. Об'єкти захисту інформації. Методи та засоби захисту інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. 2006. Вип. 2(13). С. 88-95.

7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу/ URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

Допоміжна

1. Закон України Про інформацію. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Закон України Про захист інформації в інформаційно комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/80/94 %D0%B2%D1%80#Text

3. Закон України Про захист інформації в інформаційно-комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

4. Закон України Про захист персональних даних. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf

19. Інформаційні ресурси

1. Сторінка курсу «Захист інформації» на платформі Moodle: https://dist.nupp.edu.ua/course/view.php?id=6602

2. Список нормативних документів щодо інформаційної безпеки в Україні. URL:https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BD%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B8%D1%85_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%96%D0%B2_%D1%89%D0%BE%D0%B4%D0%BE_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96