ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«___» _____ 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

АВТОМАТИЗАЦІЯ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Рівень вищої освіти	**другий (магістерський) рівень**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Предметна спеціальність (Спеціалізація) *(за наявності)*	
Освітня програма	**Системи технічного захисту інформації, автоматизація її обробки**
Статус дисципліни	**вибіркова**
Мова навчання	**українська**

Ужгород 2022

Робоча програма навчальної дисципліни «**Автоматизація обробки інформації з обмеженим доступом**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Системи технічного захисту інформації, автоматизація її обробки.**

Розробники: Чобаль О.І., к. ф.-м. н., доцент кафедри ТЕІБ

Робочу програму розглянуто та затверджено на засіданні кафедри
твердотільної електроніки та інформаційної безпеки

протокол № 7 від «28» 04 2022 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «29» 04 2022 р.

Голова науково-методичної комісії _____ Карбованець М. І.

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</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>1-й</td><td></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 – 4</td><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>Вид підсумкового контролю: залік</td><td>30</td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>72</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни **«Автоматизація обробки інформації з обмеженим доступом»** є формування у студентів компетентностей з автоматизації процесів аналізу, класифікації та обробки інформації з обмеженим доступом в умовах опрацювання значних об'ємів даних.

Завданнями даного курсу є оволодіння студентами основними методами і принципами побудови автоматизованих систем обробки інформації з обмеженим доступом, а також вільного використання організаційних, технічних та програмних методів захисту інформації під час обробки великих масивів даних.

Місце дисципліни в структурі освітньої програми: навчальна дисципліна **«Автоматизація обробки інформації з обмеженим доступом»** є вибірковим компонентом циклу професійної підготовки освітньої програми підготовки магістрів спеціальності «Системи технічного захисту інформації, автоматизація її обробки».

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

Інтегральна: здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність проводити дослідження на відповідному рівні (КЗ-2).
3. Здатність до абстрактного мислення, аналізу та синтезу (КЗ-3).
4. Здатність оцінювати та забезпечувати якість виконуваних робіт (КЗ-4).
5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності) (КЗ-5).

Фахові компетентності:

1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки (КФ1).
2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки (КФ2).
3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (КФ3).
4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог (КФ4).
5. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ6).
6. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому (КФ7).
7. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ8).

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Системи технічного захисту інформації, автоматизація її обробки»**, вивчення навчальної дисципліни **«Автоматизація обробки інформації з обмеженим доступом»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 8
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН 11
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	ПРН 16
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	ПРН 23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Автоматизація обробки інформації з обмеженим доступом»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Вміти аналізувати та оцінювати захищеність автоматизованих систем різних класів та інформації під час її автоматизованої обробки.	ПРН 6
Обґрунтовано аналізувати та оцінювати захищеність КСЗІ, КТЗІ, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Вміти розробляти і супроводжувати комплексні системи захисту інформації та системи інформаційної безпеки, а також засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 8
Забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	ПРН 11
Вміти приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 16
Обґрунтовувати вибір програмного забезпечення під час автоматизованої обробки інформації з обмеженим доступом, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань.	ПРН 23

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни **«Автоматизація обробки інформації з обмеженим доступом»** є:

- залік;
- виконання завдань лабораторних робіт;
- стандартизовані тести;
- фронтальне та/або письмове опитування

Форми контролю та критерії оцінювання результатів навчання

Модульний контроль з навчальної дисципліни **«Автоматизація обробки інформації з обмеженим доступом»** складається з поточного контролю та модульного контрольного оцінювання результатів навчання.

Форми поточного контролю:

- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- захист результатів лабораторної роботи;
- тестування;
- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів.

Форма модульного контрольного оцінювання: письмова модульна контрольна робота та/або тестування.

Форма підсумкового семестрового контролю: залік.

До заліку допускаються студенти, які відпрацювали пропущені заняття і виконали модульні контрольні роботи та завдання для самостійної роботи. Контроль самостійної роботи здійснюється шляхом перевірки виконаних завдань на лабораторних та індивідуальних заняттях, під час захисту лабораторних робіт, тестування при поточному оцінюванні, презентації результатів виконаних завдань та досліджень.

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

Поточний контроль успішності					**Модульна контрольна робота**	**Сума**
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	5	10	5	15		

Т1, Т2 ... – теми

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

Поточний контроль успішності					Модульна контрольна робота	Сума
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	10	15	5	5		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни «Автоматизація обробки інформації з обмеженим доступом»

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	3	15	5	25
Комп'ютерне тестування при тематичному оцінюванні	2	25	1	15
Модульна контрольна робота	1	60	1	60
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом відповідей на питання навчального модуля та вирішення тестових завдань. Кожна правильна відповідь оцінюється певною кількістю балів. Максимальна кількість балів за кожний модуль становить 100 балів.

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«Автоматизація обробки інформації з обмеженим доступом»** здійснюється у формі заліку, що проводиться в усній формі шляхом співбесіди. Результати заліку оцінюються за двобальною шкалою: „зараховано", „незараховано". Підсумкова оцінка визначається наступними критеріями:

Оцінка "зараховано" - якщо студент достатньо чітко і грамотно відповідає на питання в межах матеріалу, викладеного у рамках лекційних занять, може показати та обгрунтувати взаємозв'язок різних частин матеріалу, пройденого у межах матеріалу навчальної дисципліни; демонструє здатність до мислення, при відповіді на питання розмірковує, спираючись на отримані у рамках курсу знання, не допускає істотних неточностей у відповіді, правильно вибудовує логіку вирішення типових завдань;

Оцінка "незараховано" - якщо студент викладає основні питання недостатньо чітко або допускає істотні помилки при їх викладі, не може пояснити зв'язків у рамках викладеного матеріалу, не знає значної частини програмного матеріалу, не може дати точних визначень понять, пройдених у рамках курсу, дає розпливчасті формулювання і не володіє в належній мірі термінологією, плутається при відповіді на додаткові питання, не володіє прийомами вирішення типових завдань.

За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Оцінка за шкалою балів	Залік	ECTS	
		Оцінка	Характеристика
90-100	зараховано	A	відмінно
82-89		B	добре
74-81		C	добре
64-73		D	задовільно
60-64		E	задовільно
35-59	незараховано	FX	незадовільно з можливістю перескладання
1-34		F	незадовільно з обов'язковим повторним навчанням

Студент, який отримав за результатами підсумкового контролю оцінку «незараховано» або «незадовільно з обов'язковим повторним навчанням» (1-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни (під час додаткового семестру) і скласти залік або екзамен.

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. ЗАВДАННЯ, ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ АВТОМАТИЗОВАНОЇ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Тема 1. Вступ. Інформація з обмеженим доступом (ІзОД) та способи її захисту під час автоматизованої обробки

Класифікація інформації за режимом доступу: нормативно-правовий аспект. Належність інформації до ІзОД та способи її захисту. Нормативно-правові акти України, які визначають необхідність створення комплексної системи захисту інформації в ІТС.

Захист інформації в ІТС: терміни, об'єкти захисту та умови обробки інформації в системі

Захист інформації в ІТС: забезпечення захисту інформації та повноваження державних органів у сфері захисту інформації.

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та ІТС. Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Постанова КМУ № 518 від 19 червня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

Тема 2. Кіберзахист об'єктів критичної інфраструктури

Поняття об'єктів критичної інфраструктури та їх кіберзахисту

Основні вимоги щодо захисту об'єктів критичної інфраструктури: КСЗІ та система інформаційної безпеки

Завдання впровадження основних і додаткових організаційних та технічних заходів на об'єктах критичної інфраструктури

Базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури

Тема 3. Формування вимог до комплексних систем захист інформації в АС та ІТС
Автоматизовані системи (АС) обробки інформації. Класифікація АС. Обґрунтування необхідності створення КСЗІ.
Створення Служби захисту інформації (СЗІ) та вимоги щодо її складу. Положення про СЗІ в інформаційно-телекомунікаційних системах. Категоріювання об'єктів, де циркулює ІзОД. Обстеження середовищ функціонування ІТС. Обстеження обчислювальної системи та інформаційного середовища ІТС. Обстеження фізичного середовища та середовища користувачів ІТС. Акт обстеження середовищ ІТС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації.

Тема 4. Проектування системи автоматизованої обробки інформації з обмеженим доступом.
Розробка Плану захисту інформації в автоматизованих системах (АС). Формування моделі загроз для інформації в АС. Розробка моделі порушника політики безпеки АС. Система нормативних документів для забезпечення захисту інформації в автоматизованих системах. Основні вимоги та завдання загальної політики інформаційної безпеки об'єкту інформаційної інфраструктури об'єкту критичної інфраструктури.

Тема 5. Реалізація системи автоматизованої обробки інформації з обмеженим доступом.
Особливості вибору операційної системи (ОС), антивірусного програмного забезпечення (АВПЗ) і комплексу засобів захисту від НСД (КЗЗ) під час автоматизованої обробки інформації з обмеженим доступом. Вимоги до захисту інформації від НСД в АС класу «1». Мінімальний перелік функціональних послуг безпеки. Особливості організації захисту інформації від НСД в АС класу «2».

Модуль 2. ПРАКТИЧНІ АСПЕКТИ АВТОМАТИЗАЦІЇ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Тема 1. Функції та можливості програмного засобу захисту інформації «ЛОЗА™-1, версія 4» від несанкціонованого доступу в автоматизованих системах класу «1».
Основні функції програмного засобу захисту інформації від НСД «ЛОЗА™ -1, версія 4». Функціональний профіль захищеності інформації та гарантії реалізацій послуг безпеки. Порядок роботи системи. Користувачі системи. Об'єкти доступу. Правила розмежування доступу. Перевірка цілісності програмного забезпечення. Реєстрація подій.

Тема 2. Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс "Гриф" версії 5».
Основні функції та можливості засобів технічного захисту інформації від НСД «Комплекс «Гриф» версії 5». Функціональний профіль захищеності інформації та гарантії реалізацій послуг безпеки. Політика послуг безпеки, які реалізує КЗЗ. Розмежування повноважень користувачів.

Тема 3. Особливості захисту інформації в автоматизованих системах класу «2». Комплекс засобів захисту «Гриф-Мережа».
Склад та архітектура комплексу «Гриф-Мережа». Функціональний профіль захищеності інформації та гарантії реалізацій послуг безпеки. Політика послуг безпеки, які реалізує КЗЗ. Порядок роботи системи. Сервер та робочі станції. Правила розмежування доступу. Забезпечення цілісності програмного забезпечення. Реєстрація подій.

Тема 4. Автоматизація обробки інформації з обмеженим доступом засобами мови Python.
Використання базових типів та засобів мови програмування Python. Середовища та інструментарій розроблення програм мовою Python. Інтерфейс користувача IDLE. Управляючі конструкції та масиви. Обробка послідовностей при програмуванні на мові Python. Розробка програм з використанням процедур, функцій і класів Python.

Тема 5. Автоматизація роботи з файлами та створення баз даних ІзОД

Автоматизація операцій читання та запису файлів у мові Python. Особливості організації та розробки сховища даних ІзОД з використанням парадигми ООП. Під'єднання до бази даних, створення одного або декількох курсорів та виконання команди або запиту СКБД, завершення транзакції або її відкочування та закриття підключення. Редагування і видалення записів бази даних ІзОД. Основні запити СКБД SQLite.

5.2. Структура навчальної дисципліни

Денна форма навчання

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Вступ. Інформація з обмеженим доступом (ІзОД) та способи її захисту під час автоматизованої обробки	12	2		2		8
Тема 2. Кіберзахист об'єктів критичної інфраструктури	14	2		4		8
Тема 3. Формування вимог до комплексних систем захист інформації в АС та ІТС	10	2				8
Тема 4. Проектування системи автоматизованої обробки інформації з обмеженим доступом.	12			4		8
Тема 5. Реалізація системи автоматизованої обробки інформації з обмеженим доступом.	10	2				8
Модульна контрольна робота	2	2				
Разом за модуль	60	10		10		40
Модуль 2						
Тема 1. Функції та можливості програмного засобу захисту інформації «ЛОЗА™-1, версія 4» від несанкціонованого доступу в автоматизованих системах класу «1».	14	2		4		8
Тема 2. Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс "Гриф" версії 5».	12			8		4
Тема 3. Особливості захисту інформації в автоматизованих системах класу «2». Комплекс засобів захисту «Гриф-Мережа».	10	2				8
Тема 4. Автоматизація обробки інформації з обмеженим доступом засобами мови Python.	10	2		4		4
Тема 5. Автоматизація роботи з файлами та створення баз даних ІзОД	12			4		8
Модульна контрольна робота	2	2				
Разом за модуль	60	8		20		32
Разом за семестр	**120**	**18**		**30**		**72**

5.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість Годин	
		Денна	Заочна
1	Вступне заняття. Застосування термінів, визначених НД ТЗІ для підготовки документів при створенні КСЗІ	2	
2	Розробка політики інформаційної безпеки об'єкту критичної інфраструктури	4	
3	Модель порушника безпеки автоматизованої системи. План захисту інформації в автоматизованій системі	4	
4	Обов'язки системного адміністратора КЗЗ «Гриф»	4	
5	Інсталяція комплексу засобів захисту «Гриф»	4	
6	Функціональні характеристики комплексу засобів захисту «Лоза-1»	4	
7	Використання базових типів та засобів мови програмування Python. Середовища та інструментарій розроблення програм мовою Python	4	
8	Автоматизоване створення баз даних та робота з файлами у мові Python	4	
	Разом	**30**	

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Головні принципи та етапи захисту інформації від загроз	4	
2.	Нормативно-правові акти України, які визначають необхідність створення КСЗІ в ІТС	4	
3.	Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак	4	
4.	Категоризація об'єктів критичної інфраструктури. Методичні рекомендації Держспецзв'язку	4	
5.	Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури	4	
6.	Базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури. Загальна політика інформаційної безпеки	4	
7.	Основні принципи забезпечення інформаційної безпеки в автоматизованих системах	4	
8.	Функції служби захисту інформації щодо обробки інформації з обмеженим доступом в автоматизованих системах	4	
9.	Зміст плану захисту інформації з обмеженим доступом в автоматизованих системах	4	
10.	Побудова систем захисту від загрози порушення конфіденційності інформації: вимоги до вибору паролів і параметри для кількісної оцінки стійкості парольних систем захисту	4	
11.	Загальна характеристика криптографічних методів захисту інформації в автоматизованих системах	4	
12.	Особливості банківських систем автоматизованого документообігу	4	

13.	Використання систем автоматизованого документообігу органами державної влади та місцевого самоврядування	4	
14.	Особливості систем автоматизованого документообігу в аптеках і лікарських установах	4	
15	Використання комплексів засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу до інформації під час її автоматизованої обробки	4	
16	Розробка програм з ієрархією класів. Організація класів з використанням успадкування в Python	4	
17	Використання фреймворків для створення, інтеграції та доступу до баз даних засобами мови Python	4	
18	Розроблення програмного забезпечення з графічним інтерфейсом мовою Python	4	
	Разом	**72**	

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

Технічні засоби: технічні засоби навчання, зокрема мультимедійний проектор.
Обладнання: персональні комп'ютери з можливістю доступу в Інтернет.
Програмне забезпечення: інтерпретатор Python, IDLE

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Комплексні системи захисту інформації : навчальний посібник/ К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018.– 118 с
2. В. Гребенніков. Комплексні системи захисту інформації. Проектування, впровадження, супровід. Вид. Litres, 2022
3. Захист інформації в автоматизованих системах управління: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с
4. Організація захисту інформації з обмеженим доступом: навч. посіб./А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. – К.: Нац. акад., СБУ, 2018. –252 с.
5. Копей В.Б. Мова програмування Python для інженерів і науковців: Навчальний посібник. Івано-Франківськ : ІФНТУНГ, 2019. 274с.

Допоміжна література

1. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
2. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
3. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.Leach A.R..

Інформаційні ресурси в мережі Інтернет

1. http://avtoprom.kiev.ua/avtoprom/ua/content/Система-захисту-інформації-ЛОЗА™-1-версія-4
2. http://www.ict.com.ua/?lng=1&sec=8&art=41
3. http://www.ict.com.ua/files/grif/gm_3_op_ukr.pdf
4. https://www.python.org/downloads/