МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«13» 06 2024р

ЗАТВЕРДЖУЮ:
Директор навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«30» 08 2024р.

РОБОЧА ПРОГРАМА
з дисципліни
«МОНІТОРИНГ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

Ступінь вищої освіти – **магістр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека та захист інформації**
Освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. роб. (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом	Екзамен
ДФН	1	1	30	14	4	6	96	150	1
ЗФН	1	1	8	4			138	150	2

30.08.2024р.

Тернопіль – 2024

Робоча програма складена на основі освітньо-професійної програми підготовки магістра галузі знань 12 Інформаційні технології, спеціальність 125 – Кібербезпека та захист інформації, затвердженої на засіданні Вченою радою ЗУНУ, протокол № 11 від 26.06.2024р.

Робочу програму склав доцент кафедри кібербезпеки, к.т.н., доцент Степан ІВАСЬЄВ

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 1 від 26.08.2024 р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол №1 від 30.08.2024 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни "Моніторинг та управління інформаційною безпекою"

Дисципліна – Моніторинг та управління інформаційною безпекою	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань 12 -Інформаційні технології	Статус дисципліни - обов'язкова Мова навчання – українська
Кількість залікових модулів – 4	Спеціальність - 125 Кібербезпека та захист інформації	Рік підготовки: ДФН – 1; ЗФН - 1 Семестр: ДФН – 1; ЗФН – 1, 2
Кількість змістових модулів – 3	Ступінь вищої освіти – магістр	Лекції : ДФН – 30 год.; ЗФН – 8 год. Практичні заняття : ДФН – 14 год.; ЗФН – 4 год.
Загальна кількість годин – 150		Самостійна робота: ДФН – 96 год. ЗФН – 138 год. Тренінг: ДФН - 6 год. Індивідуальна робота: ДФН - 4 год.
Тижневих годин: 10год., з них аудиторних - 3 год.		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни «Моніторинг та управління інформаційною безпекою»

2.1. Мета завдання дисципліни

Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області інформаційної безпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних системах та мережах.

Метою викладання дисципліни є розкриття сучасних методів захисту інформації в комп'ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

2.2. Завдання вивчення дисципліни

Завданнями вивчення навчальної дисципліни є:

- реалізація захисту конфіденційності інформації;
- здійснення захисту цілісності інформації;
- сприяння доступності необхідної інформації.

Завдання лекційних занять включає вивчення основних теоретичних понять та принципів, пов'язаних із моніторингом та управлінням інформаційною безпекою, а також аналіз сучасних викликів та стратегій в цій галузі.

Завдання проведення Проведення практичних занять спрямоване на формування у студентів практичних навичок з моніторингу та управління інформаційною безпекою, включаючи вирішення реальних завдань та використання інструментів і методів для забезпечення безпеки даних та інформаційних систем.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

Здатність до абстрактного мислення, аналізу та синтезу.

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.

Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних

процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Моніторинг та управління інформаційною безпекою» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів спеціальності «Кібербезпека» ступена вищої освіти бакалавр, зокрема «Кібернетична безпека», «Безпека комп'ютерних мереж», «Безпека Web-ресурсів», «Криптографія» та ін, а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів

2.5. Результати навчання

В результаті вивчення дисципліни студенти повинні отримати теоретичні знання, вміння та навики для вибору щодо моніторингу інформаційної безпеки та практичні навики використання сучасних засобів управління інформаційної безпеки, зокрема:

Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації

Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

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.

3. Програма навчальної дисципліни

Змістовий модуль 1. Захист комп'ютерних систем.

Тема 1. Постановка задачі аналізу захищеності комп**'**ютерної системи. Методи виявлення вразливостей системи аналізу. Література, методичні рекомендації щодо дисципліни.

Література: 2, 6.

Тема 2. Мережеві сканери безпеки. Способи збору інформації про мережу.

1. Розміщення мережевих агентів сканування в мережі. 2. Мережеві агенти і збір інформації. 3. Попереднє вивчення цілі. 4. Способи збору інформації про мережу. 5. Поняття ключової інформації та види носіїв для її зберігання (дискети, електронні ключі, SMART-карти, пристрої Touch-Memory).

Література: 3, 7.

Змістовий модуль 2. Захищені віртуальні мережі та протоколи безпеки.

Тема 3. Ідентифікація мережевих об'єктів. Визначення топології мережі.

1. Використання протоколу ICMP. 2. Ідентифікація вузлів з допомогою протоколу ARP. 3. Відслідковування маршрутів. Відслідковування маршрутів і фільтрація. 4. Утиліта traceproto.

Література: 2, 5.

Тема 4. Ідентифікація статусу апорта, сервісів та додатків. Ідентифікація операційних систем.1. Сканування портів. 2. Сканування портів TCP - служб. 3. Сканування портів UDP - служб. 4. Ідентифікація TCP – служб, UDP - служб. 5. Сканування протоколів. 6. Прості методи визначення ОС. 7. Опитування стеку TCP/IP. 8. Інструменти, SinFP. 9. Використання протоколу ICMP. 10. Port 0 OS Fingerprinting. 11. Активна ідентифікація ОС – перспективи.

Література: 2, 6.

Змістовий модуль 3. Ідентифікація вразливостей по дотичних ознаках.

Тема 5. Методи ідентифікації вразливостей по дотичних ознаках. Passive Fingerprinting.

1. Банерні перевірки. 2. Мережеві сервіси як обєкти сканування. Локальні перевірки. 2 Механізми взаємодії з системами Windows. 3. Стек протоколів TCP/IP. 4. Проблеми безпеки IP-мереж. IP версія 4. IP версія 6. 5. Аналіз мережевого трафіку. Аналіз запитів від вузла який сканується.

Література: 3, 6.

Тема 6. Виявлення вразливостей за допомогою тестів. Мережевий сканер Nessus.

1. Експлойти і їх різновиди. Використання техніки запуску коду. 2. Прості екплойти. Віддалений підбір паролю. Оцінка стійкості паролів. Тестування. 3. Огляд можливостей сканера. 4. Архітектура сканера. 5. Отримання та встановлення сканера. Робота зі сканером.

Література: 1, 8.

Тема 7. Мова опису атак NASL.

1. Структура сцерарію. 2. Синтаксис мови і бібліотеки, які підкулючаються.

Література: 2, 6.

Тема 8. Сканери безпеки компанії Positive Technologies.

1. Архітектура і основні можливості сканера XSpider. 2. Етапи роботи сканера XSpider. 3. Збір інформації про мережу. 4. Ідентифікація вразливостей. Локальні перевірки Windows. 5. Виявлення вразливостей web-додатків.

Література 3-5

Тема 9. Аналіз захищеності на рівні вузла. Спеціалізовані засоби аналізу захищеності.

1. Задачі локального сканування. Архівтектура. 2. Збір інформації і ідентифікація вразливостей. 3. Сканер Assuria Auditor. 4. Класифікація сканерів безпеки по призначенню. 5. Загрози і вразливості СУБД. Приклади програм-сканерів вразливостей СУБД.

Література 3-5

Тема 10. Методологія аналізу захищеності Ethical Hacking. Централізоване управління вразливостями.

1. Необхідність методології аналізу захищеності. 2. Penetration Testing – загальні відомості. Структура Penetration Testing. 3. Необхідність централізованого управління вразливостей. 4. Інвентаризація інформаційних активів. 5. Моніторинг стану захищеності.

Література 3-5

Тема 11. Контроль захищеності безпровідних мереж.

1. Особливості сканування безпровідних мереж. 2. Сканери для безпровідних мереж. 3. Сканування точки доступу на мережевому рівні. 4. Методологія аудиту. 5. Загрози, повязані з використанням безпровідних мереж. 6. IEEE 802.11i – невирішені проблеми.

Література 3-5

Тема 12. Виявлення атак на безпровідні мережі.

1. Несанкціоноване використання безпровідних засобів. 2. Атаки на пристрої та і сервіси. 3. Атаки на механізм аутентифікації 802.1x. 4. Атаки на клієнтів. 5. Моніторинг безпеки. 6. Особливості виявлення атак. 7. Атаки, характерні для безпровідних мереж.

Література 1-7

Тема 13. Джерела даних для систем виявлення атак.

1. Складові технології виявлення атак. 2. Мережевий трафік як джерело даних. Виявлення атак на рівні вузла. 3. Host IDS – контроль дій суб'єктів системи. 4. Складові виявлення атак рівня вузла.

Література 3-5

Тема 14. Признаки атак. Методи виявлення атак.

1. Аналіз даних про потік. 2. Використання вразливостей як признаків атак. 3. Відхилення від порогових значень. 4. Система виявлення атак Snort.

Література 1-5

Тема 15. Інтеграція засобів виявлення і запобігання атак в єдину систему і взаємозвязок з іншими засобами захисту.

1. Інтеграція засобів виявлення і запобігання атак в єдину систему. 2. Приклади кореляції даних.

Література 3-5

4. Структура залікового кредиту дисципліни

4.1 Структура залікового кредиту дисципліни (денна форма навчання)

	Кількість годин					
	Лекції	Практ. заняття	ІРС	Тренінг	СРС	Контрольні заходи
Змістовий модуль 1. Захист комп'ютерних систем						
Тема 1. Постановка задачі аналізу захищеності комп'ютерної системи. Методи виявлення вразливостей системи аналізу. Література, методичні рекомендації щодо дисципліни.	2		1	2	5	Поточне опитування
Тема 2. Мережеві сканери безпеки. Способи збору інформації про мережу. Попереднє вивчення цілі	2	2			5	
Змістовий модуль 2. Захищені віртуальні мережі та протоколи безпеки						
Тема 3. Ідентифікація мережевих об'єктів. Визначення топології мережі	2		1	2	5	Поточне опитування
Тема 4. Ідентифікація статусу апорта, сервісів та додатків. Ідентифікація операційних систем.	2	2			5	
Змістовий модуль 3. Сучасні криптографічні протоколи та методи криптоаналізу						
Тема 5 Методи ідентифікації вразливостей по дотичних ознаках. Passive Fingerprinting.	2		2	2	5	Поточне опитування
Тема 6. Виявлення вразливостей за допомогою тестів. Мережевий сканер Nessus	2	2			5	
Тема 7. Мова опису атак NASL.	2	2			5	
Тема 8. Сканери безпеки компанії Positive Technologies	2				5	
Тема 9. Аналіз захищеності на рівні вузла. Спеціалізовані засоби аналізу захищеності	2	2			8	
Тема 10. Методологія аналізу захищеності Ethical Hacking. Централізоване управління вразливостями.	2	2			8	
Тема 11. Контроль захищеності безпровідних мереж.	2	2			8	
Тема 12. Виявлення атак на безпровідні мережі	2				8	
Тема 13. Джерела даних для систем виявлення атак.	2				8	
Тема 14. Признаки атак. Методи виявлення атак	2				8	
Тема 15. Інтеграція засобів виявлення і запобігання атак в єдину систему і взаємозвязок з іншими засобами захисту.	2				8	
Разом	**30**	**14**	**4**	**6**	**96**	

4.2 Структура залікового кредиту (заочна форма навчання)

	Кількість годин				
	Лекції	Практ. заняття	ІРС	СРС	Контрольні заходи
Змістовий модуль 1. Захист комп'ютерних систем					
Тема 1. Постановка задачі аналізу захищеності комп'ютерної системи. Методи виявлення вразливостей системи аналізу. Література, методичні рекомендації щодо дисципліни.	0,5			7	Поточне опитування
Тема 2. Мережеві сканери безпеки. Способи збору інформації про мережу. Попереднє вивчення цілі	0,5	0,5		7	
Змістовий модуль 2. Захищені віртуальні мережі та протоколи безпеки					

Тема 3. Ідентифікація мережевих об'єктів. Визначення топології мережі	0,5			7	Поточне опитування
Тема 4. Ідентифікація статусу апорта, сервісів та додатків. Ідентифікація операційних систем.	0,5	0,5		7	
Змістовий модуль 3. Сучасні криптографічні протоколи та методи криптоаналізу					
Тема 5 Методи ідентифікації вразливостей по дотичних ознаках. Passive Fingerprinting.	0,5			10	Поточне опитування
Тема 6. Виявлення вразливостей за допомогою тестів. Мережевий сканер Nessus	0,5	0,5		10	
Тема 7. Мова опису атак NASL.	0,5	0,5		10	
Тема 8. Сканери безпеки компанії Positive Technologies	0,5			10	
Тема 9. Аналіз захищеності на рівні вузла. Спеціалізовані засоби аналізу захищеності	1	0,5		10	
Тема 10. Методологія аналізу захищеності Ethical Hacking. Централізоване управління вразливостями.	0,5	0,5		10	
Тема 11. Контроль захищеності безпровідних мереж.	0,5			10	
Тема 12. Виявлення атак на безпровідні мережі	0,5	0,5		10	
Тема 13. Джерела даних для систем виявлення атак.	0,5			10	
Тема 14. Признаки атак. Методи виявлення атак	0,5	0,5		10	
Тема 15. Інтеграція засобів виявлення і запобігання атак в єдину систему і взаємозвязок з іншими засобами захисту.	0,5			10	
Разом	8	4		138	

5. Тематика практичних занять

Практична робота №1.

Тема: Апаратна побудову захисту на основі BIOS.

Мета: Виконання роботи з налаштування BIOS в частині парольного захисту.

Питання для обговорення: основні поняття та визначення.

Література: 2, 4.

Практична робота №2.

Тема: Програмна побудову захисту на основі BIOS.

Мета: Ознайомлення з програмними побудови захисту на основі BIOS.

Питання для обговорення: основні поняття та визначення.

Література: 2, 3.

Практична робота №3.

Тема: Механізм зараження комп'ютера adware- та spyware- програмами, комп'ютерними вірусами тощо та протидію цим процесам

Мета: Вивчення механізму зараження комп'ютера adware- та spyware- програмами, комп'ютерними вірусами.

Питання для обговорення: основні поняття та визначення.

Література: 1, 3.

Практична робота №4.

Тема: Дослідження процедури шифрування та дешифрування в в асиметричних криптосистемах.

Мета: Оволодіння методами для шифрування та дешифрування в криптосистемі RSA.

Питання для обговорення: основні поняття та визначення.

Література: 2, 4.

Практична робота №5.

Тема: Побудова захищених віртуальних мереж за допомогою міжмережевих екранів

Мета: Вивчення та дослідження побудови захищених віртуальних мереж за допомогою міжмережевих екранів

Питання для обговорення: основні поняття та визначення.

Література: 3, 4.

6. Самостійна робота

Самостійна робота з курсу «Моніторинг та управління інформаційною безпекою» виконується самостійно студентом на одного основі сформованого завдання, яке охоплює основні теми курсу. Орієнтовні варіанти завдань з дисципліни «Моніторинг та управління інформаційною безпекою»:

- Предмет дисципліни, її структура, задачі і форми контролю, основна література.
- Огляд методів та засобів захисту комп'ютерних систем.
- Класифікація методів та засобів захисту інформації.
- Захист комп'ютерних систем шляхом блокування доступу до них.
- Проблеми безпеки в Інтернет.
- Криптосистеми Рабіна та Ель–Гамаля.
- Проблеми безпеки корпоративних інформаційних систем.
- Побудова підсистеми інформаційної безпеки.
- Побудова підсистеми інформаційної безпеки.
- Принципи інформаційної безпеки.
- Особливості міжмережевого екранування на різних рівнях моделі OSI.
- Побудова захищених віртуальних мереж VPN.
- Розподіл криптографічних ключів.
- Безпека віддаленого доступу до комп`ютерної мережі.

8. Організація та проведення тренінгу

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.

3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Рекомендується наступне проведення тренінгу:

1. Огляд сучасних програмних середовищ для вирішення задач моніторингу мережевої безпеки: розгляд сучасних програмних середовищ для вирішення задач комп’ютерної криптографії; вивчення можливостей сучасних програмних середовищ для вирішення задач комп’ютерної криптографії.

2. Розгляд процесу програмної реалізації криптографічних алгоритмів: постановка задачі; опис технічного завдання; програмна реалізація криптографічних алгоритмів.

3. Розв’язування наскрізних задач, що охоплюють усі розділи дисципліни «Моніторинг мережевої безпеки »: опис наскрізної задачі шифрування; розбиття задачі на окремі підзадачі; об’єднання розв’язаних підзадач в єдине ціле з метою вирішення усієї задачі.

Орієнтовна тематика завдань:

1. Розробка та аналіз простих криптографічних алгоритмів на основі методів перестановок та підстановок.

2. Генерація псевдовипадкових послідовностей чисел в системах захисту інформації.

3. Оцінка статистичних характеристик датчика псевдовипадкових чисел із заданим законом розподілу.

4. Розробка і реалізація варіанта симетричного криптографічного алгоритму з DES – подібною структурою.

4. Оцінка швидкості роботи криптоалгоритму.

5. Розробка алгоритму та програмна реалізація атаки на симетричну криптосистему.

6. Програмна реалізація алгоритму RSA.

7. Розробка і програмна реалізація протокола обміну симетричними ключами на

основі алгоритму Diffyie-Hellman.

8. Розробка і програмна реалізація алгоритму обчислення цифрового дайджеста повідомлення.

9. Програмна реалізація алгоритмів цифрового підпису.

10. Схема режиму шифрування DES-ECB.

11. Схема режиму шифрування DES-CBC.

12. Схема режиму шифрування DES-CPB и DES-OFB.

13. Потрійний DES. Сфери застосування різних режимів DES.

14. Схема режиму шифрування простої заміни ГОСТ 28147-89.

15. Реалізація алгоритму шифрування RSA.

16. Реалізація алгоритму шифрування Ель-Гамаля.

17. Алгоритм шифрування на основі задачі про укладку портфеля.

18. Реалізація алгоритму шифрування на основі еліптичних кривих.

19. Реалізація основних хеш-функцій.

20. Реалізація хеш-функції. MD5.

21. Реалізація основних криптографічних протоколів.

22. Реалізація протоколів обміну ключами.

23. Реалізація протоколів аутентифікації.

24. Реалізація парольної ідентифікації/аутентифікації.

25. Реалізація протоколу ідентифікації/аутентифікації на основі шифрування з відкритим ключем.

26. Сервер аутентифікації Kerberos.

27. Ідентифікація/аутентифікація з допомогою біометричних даних.

28. Реалізація електронного цифрового підпису.

29. Реалізація ЕЦП на базі алгоритму RSA.

30. Реалізація ЕЦП на базі алгоритму DSA.

31. Реалізація алгоритму цифрового підпису ГОСТ 34.10-94.

32. Реалізація алгоритму цифрового підпису ГОСТ 34.10-2001.

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Моніторинг та управління інформаційною безпекою» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;

– поточне опитування;

- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи.
- екзамен.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальної шкалою) з дисципліни «Моніторинг та управління інформаційною безпекою» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%

Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях 1-5.	Підсумкова письмова робота за темами №1-15.	Оцінка за виконання одного завдання тренінгу	Оцінка за виконання одного завдання самостійної роботи	Теоретичні питання: 2 питання по 30 балів. Практичне завдання 40 балів

Шкала оцінювання

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90-100	Відмінно	A (відмінно)
85-89	Добре	B (дуже добре)
75-84		C (добре)
65-74	Задовільно	D (задовільно)
60-64		E (достатньо)
35-59	Незадовільно	FX (незадовільно, з можливістю повторного складання)
1-34		F (незадовільно, з обов'язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна.

№	Найменування	№теми
1	Опорний конспект лекцій з дисципліни «Моніторинг мережевої безпеки»	1-15
2	Методичні вказівки до виконання лабораторних робіт з дисципліни «Моніторинг мережевої безпеки»	1-5
3	Обладнання: Проектор, комп'ютери з доступом до мережі Інтернету. Програмне забезпечення: FoxitReader, WinZip, Total Commander, Dev C++, Python 3.5.8, Ubuntu 19.04	1-5

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Soni, Arun. The Cybersecurity Self-Help Guide. CRC Press, 2021.
2. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021,13,39. https://doi.org/ 10.3390/fi13020039
3. ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
4. Wangen, G. Quantifying and Analyzing Information Security Risk from Incident Data; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019, pp. 129–154.
5. Radanliev P., et al. "Cyber Risk in IoT Systems." (2019).
6. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." Future Internet 12.9, 2020: 157.
7. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
8. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
9. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 с.
10. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
11. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p