

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

**ЗАТВЕРДЖУЮ**

Декан ФКІТ  
Ігор ЯКИМЕНКО

  
«30» 2024 р.

**ЗАТВЕРДЖУЮ**

Проректор з науково-педагогічної роботи  
Віктор ОСТРОВЕРХОВ


  
«30» 2024 р.

**РОБОЧА ПРОГРАМА**

з дисципліни «Кібернетична безпека»  
ступінь вищої освіти – бакалавр  
галузь знань - 12 Інформаційні технології  
спеціальність – 125 Кібербезпека  
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	3	5	46	44	5	12	73	180	5

30.08.2024  


Тернопіль –2024

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», затвердженої Вченою радою ЗУНУ (протокол № 9 від 15.06.2022 р.).

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків

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 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2024 р.

Голова групи  
забезпечення спеціальності



Василь ЯЦКІВ

Гарант освітньо-професійної  
програми



Михайло КАСЯНЧУК

## СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### 1. Опис дисципліни «Кібернетична безпека»

Дисципліна «Кібернетична безпека»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 6	Галузь знань 12 Інформаційні технології	<b>Статус дисципліни:</b> обов'язкова <b>Мова навчання:</b> українська
Кількість залікових модулів – 5	Спеціальність 125 «Кібербезпека»	Рік підготовки: Денна – 3 Семестр: Денна – 5
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: 46 год. Лабораторні заняття: 44 год.
Загальна кількість годин – 180		Самостійна робота: 73 год. Тренінг: 12 год. Індивідуальна робота: 5 год.
Тижневих годин – 12, з них аудиторних – 6		Вид підсумкового контролю – екзамен

### 2. Мета і завдання дисципліни «Кібернетична безпека»

#### 2.1. Мета вивчення дисципліни

Метою дисципліни «Кібернетична безпека» є - отримання знань та навичок, необхідних для успішного виконання завдань аналітика, який працює в центрі моніторингу та управління безпекою (SOC).

#### 2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку, зокрема: аналізувати роботу мережевих протоколів і служб; класифікувати різні типи мережевих атак; використовувати засоби мережевого моніторингу для визначення атак на мережеві протоколи і служби; застосовувати різні способи запобігання несанкціонованому доступу до комп'ютерних мереж, хостів і даними; виявляти попередження безпеки мережі; аналізувати дані про вторгнення в мережу для перевірки потенційних загроз; застосовувати моделі реагування для усунення інцидентів безпеки.

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

Знання та розуміння предметної області та розуміння професії.

Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з

встановленою політикою інформаційної та/або кібербезпеки.

#### **2.4. Передумови для вивчення дисципліни**

Перелік дисциплін, які мають бути вивчені раніше: програмування на мові Python; Кібернетична безпека; Операційні системи; Алгоритми та структури даних; Архітектура комп'ютерів та систем.

Перелік раніше здобутих результатів навчання: використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Розробляти моделі загроз та порушника; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах.

#### **2.5. Результати навчання**

Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах;

Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів.

### **3. Програма навчальної дисципліни: «Кібернетична безпека»**

#### ***Змістовий модуль 1. Типи комп'ютерних атак***

##### ***Тема 1. Кібербезпека і центр моніторингу та управління безпекою.***

Історії битв. Зловмисники. Злом особистих даних. Борці з кіберзлочинністю. Сучасний центр моніторингу та управління безпекою (SOC). Елементи SOC. Люди в SOC. Технології в SOC.

Література: 1, 2, 3, 4.

##### ***Тема 2. Принципи забезпечення безпеки комп'ютерних систем.***

Хакери і їх інструменти. Хто атакує наші мережі? Кіберзлочинці. Загрози, уразливості і ризики. Завдання кібербезпеки.

Література: 1, 2, 4, 8.

##### ***Тема 3. Поширені атаки на комп'ютерні системи.***

Шкідливе ПЗ. Типи шкідливого ПЗ. Віруси. Трояні. Класифікація троянів. Типи мережових атак. Віруси вимагачі.

Література: 1, 2, 6, 7

##### ***Тема 4. Типи атак на комп'ютерні системи.***

Розвідка. Атаки доступу. Типи атак доступу. Атаки методом соціальної інженерії. DDoS- атаки.

Література: 1, 2, 5, 7.

##### ***Тема 5. Моніторинг мережі і засоби моніторингу.***

Топологія мережевої безпеки. Методи моніторингу мережі. Відгалуження мережі. Зеркалювання трафіку і аналізатор комутованих портів. Засоби моніторингу мережевої активності. Аналізатори мережових протоколів. NetFlow. Системи SIEM.

Література: 1, 2, 5, 9.

**Тема 6. Атаки на базові функції.**

Загрози і вразливості. Вразливості IP. Атаки на основі ICMP. Атаки типу відмова в обслуговуванні (DoS -атаки). DDoS - атаки. Атаки з підміною адресу.

Література: 1, 2, 7, 9.

**Тема 7. Атаки на службові протоколи.**

Вразливості ARP. Підробка записів хешу ARP. Атаки DNS. Тунелювання DNS. DHCP. Протоколи HTTP і HTTPS. Бази даних з веб-доступом.

Література: 1, 2, 4, 10

**Змістовий модуль 2. Моніторинг безпеки.**

**Тема 8. Захист мережі.**

Ідентифікація ресурсів. Виявлення вразливостей. Визначення загроз. Політики безпеки. Бізнес - політики. Політика BYOD. Відповідність нормативним вимогам і стандартам.

Література: 1, 4, 6.

**Тема 9. Управління доступом.**

Концепції управління доступом. Моделі управління доступом. Функціонування AAA. Автентифікація AAA. Служби аналітики загроз. Cisco Talos. FireEye. Автоматизована система обміну індикаторами. База вразливостей CVE.

Література: 1, 4, 10.

**Тема 10. Захист кінцевих пристроїв.**

Захист від вторгнення на рівні хоста. Безпека додатків. Оцінка вразливостей кінцевих пристроїв. Загальна система оцінки вразливостей. Безпечне управління пристроями. Системи управління інформаційною безпекою.

Література: 1, 4, 7, 9.

**Тема 11. Моніторинг безпеки.**

Моніторинг загальних протоколів. Технології забезпечення безпеки. Файли журналів. Журнали кінцевих пристроїв. Мережеві журнали.

Література: 1, 4, 6, 10

**Тема 12. Аналіз даних вторгнень.**

Оцінка попереджень. Робота з даними безпеки мережі. Дослідження мережевих даних. Цифрова технічна експертиза. Порядок збору доказів.

Література: 1, 4, 11

**Тема 13. Реагування на інциденти і їх обробка.**

Моделі реагування на інциденти. Ланцюг кібервбивства. Ромбовидна модель вторгнення. Схема VERIS.

Література: 1, 2, 5.

**Тема 14. Обробка інцидентів.**

Типи груп CSIRT. CERT. Життєвий цикл реагування на інциденти NIST. Виявлення і аналіз. Дії після інцидентів. Збір і зберігання даних про інциденти.

Література: 1, 3, 4, 12

#### 4. Структура залікового кредиту з дисципліни «Кібернетична безпека»

	Кількість годин					
	Лекції	Прак-тичні заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Типи комп'ютерних атак.						
Тема 1. Кібербезпека і центр моніторингу та управління безпекою.	2	2	4	2	6	Поточне опитування
Тема 2. Принципи забезпечення безпеки комп'ютерних систем.	4	2	4			
Тема 3. Поширені атаки комп'ютерні системи.	2	2	5			
Тема 4. Типи атак на комп'ютерні системи	4	4	6			
Тема 5. Моніторинг мережі і засоби моніторингу.	2	2	6			
Тема 6. Атаки на базові функції.	2	2	5			
Тема 7. Атаки на службові протоколи.	2	2	5			
Змістовий модуль 2. Моніторингу та управління безпекою.						
Тема 8. Захист мережі.	4	4	5	3	6	Поточне опитування
Тема 9. Управління доступом.	2	4	5			
Тема 10. Захист кінцевих пристроїв.	4	4	5			
Тема 11. Моніторинг безпеки.	4	4	6			
Тема 12. Аналіз даних вторгнень.	4	4	6			
Тема 13. Реагування на інциденти і їх обробка.	4	4	6			
Тема 14. Обробка інцидентів.	2	4	5			
Разом	46	44	73	5	12	

## **5. Тематика практичних (семінарських або лабораторних) занять**

### **Лабораторна робота №1**

Тема: Вивчення процесів, потоків, дескрипторів і реєстру Windows

Мета: вивчення процесів, потоків і дескриптори за допомогою засобу Process Explorer, що входить до складу SysInternals Suite.

Питання для обговорення:

1. Вивчення процесів
2. Вивчення потоків і дескрипторів
3. Вивчення реєстру Windows

Література: 1, 2.

### **Лабораторна робота №2**

Тема: Аналіз трафіку HTTP і HTTPS за допомогою програми Wireshark

Мета: навчитися аналізувати і перехоплювати трафік HTTP і HTTPS за допомогою програми Wireshark.

Питання для обговорення:

1. Перехоплення і перегляд HTTP-трафіку
2. Перехоплення і перегляд HTTPS-трафіку

Література: 1, 2.

### **Лабораторна робота №3**

Тема: Packet Tracer. Наочне подання роботи списку контролю доступу

Мета: навчитися використовувати список контролю доступу (ACL) для заборони ехозапитів, відправлених на вузли віддалених мереж.

Питання для обговорення:

1. Перевірка локального підключення і тестування роботи списку контролю доступу
2. Видалення списку контролю доступу та перевірка підключення

Література: 1, 2.

### **Лабораторна робота №4**

Тема: Packet Tracer. Визначення потоку пакетів

Мета: спостереження за потоком пакетів в топології локальної та глобальної мережі а також спостереження за змінами потоку пакетів при зміні топології мережі.

Питання для обговорення:

1. Перевірка зв'язку
2. Топологія віддаленої локальної мережі
3. Топологія глобальної мережі

Література: 1, 2.

### **Лабораторна робота №5**

Тема: Packet Tracer. Ведення журналу мережевої активності

Мета: навчитися використовувати Packet Tracer для аналізу і реєстрації мережевого трафіку. Ви розглянете вразливість в одному мережевому додатку, а також перегляньте трафік ICMP за допомогою системного журналу.

Питання для обговорення:

1. Створення трафіку FTP
2. Вивчення трафіку FTP
3. Перегляд повідомлень системного журналу

Література: 1, 2.

### **Лабораторна робота №6**

Тема: Вивчення трафіку DNS

Мета: навчитися використовувати програму Wireshark в системі Windows для фільтрації пакетів DNS і перегляду інформації як про пакети запитів, так і відповідей DNS.

Питання для обговорення:

1. Перехоплення трафіку DNS
2. Вивчення трафіку DNS-запиту
3. Вивчення трафіку DNS-відповіді

Література: 1, 2.

#### **Лабораторна робота №7**

Тема: Читання журналів сервера

Мета: вивчення журналів сервера

Питання для обговорення:

1. Читання файлів журналів з використанням програм Cat, More і Less
2. Файли журналів і Syslog
3. Файли журналів і Journalctl

Література: 1, 2.

#### **Лабораторна робота №8**

Тема: Вивчення сеансів зв'язку за протоколами Telnet і SSH за допомогою програми Wireshark

Мета: навчитися налаштовувати маршрутизатор для підключень по протоколу SSH і використовувати програму Wireshark для перехоплення і перегляду даних, що передаються під час сеансів Telnet і SSH.

Питання для обговорення:

1. Вивчення сеансу Telnet за допомогою програми Wireshark
2. Вивчення сеансу SSH за допомогою програми Wireshark

Література: 1, 2.

#### **Лабораторна робота №9**

Тема: Дослідження реалізації NetFlow

Мета: використання Packet Tracer для створення мережевого трафіку і спостереження за відповідними записами потоків NetFlow в засобі збору даних NetFlow..

Питання для обговорення:

1. Спостереження за записом потоків NetFlow (один напрямок).
2. Спостереження за записом потоків NetFlow для сеансу, який входить в засіб збору даних і виходить з нього.

Література: 1, 2.

#### **Лабораторна робота №10**

Тема: Packet Tracer. Ведення журналів з декількох джерел завдання

Мета: навчитися використовувати Packet Tracer для перегляду даних, сформованих системним журналом, AAA і NetFlow.

Питання для обговорення:

1. Використання системного журналу для перехоплення файлів з декількох мережевих пристроїв
2. Спостереження за доступом користувача AAA
3. Ознайомлення з інформацією про NetFlow.

Література: 1, 2.

#### **Лабораторна робота №11**

Тема: Налаштування середовища з кількома VM

Мета: навчитися налаштовувати середовище віртуальної мережі шляхом підключення один до одної декількох віртуальних машин в Virtualbox.

Питання для обговорення:



1. Імпорт пристрою віртуальної машини в VirtualBox
  2. Об'єднайте в мережу віртуальні машини для створення віртуальної лабораторної середовища
  3. Завершення роботи віртуальних машин.
- Література: 1, 2.

### **Лабораторна робота №12**

**Тема:** Правила Snort і міжмережевого екрану

**Мета:** Ознайомлення з принципами написання правил Snort і міжмережевого екрану

**Питання для обговорення:**

1. Підготовка віртуального середовища
2. Брандмауер і журнали IDS
3. Завершення і очищення процесу Mininet

Література: 1, 2.

### **Лабораторна робота №13**

**Тема:** Перетворення даних в універсальний формат

**Мета:** навчити студентів, як знаходити місце зберігання файлів журналів, а також як управляти ними і переглядати їх.

**Питання для обговорення:**

1. Нормалізація мітки часу в файлі журналу.
2. Нормалізація мітки часу в файлі журналу Apache
3. Підготовка файлу журналу в Security Onion

Література: 1, 2.

### **Лабораторна робота №14**

**Тема:** Витягування виконаного файлу з PCAP

**Мета:** Навчитися аналізувати трафік в раніше перехопленому файлі PCAP і витягувати виконуваний файл з файлу а також розуміння виконання мережевих транзакцій на рівні пакетів.

**Питання для обговорення:**

1. Підготовка віртуального середовища.
2. Аналіз попередньо записаних журналів і перехоплень трафіку.

Література: 1, 2.

### **Лабораторна робота №15**

**Тема:** Інтерпретація даних HTTP і DNS для ізоляції хакера

**Мета:** навчитися відслідковувати по журналам використання відомих вразливостей DNS і HTTP.

**Питання для обговорення:**

1. Підготовка віртуального середовища.
2. Вивчення атаки на основі впровадження шкідливого коду SQL.
3. Аналіз крадіжки даних.

Література: 1, 2.

### **Лабораторна робота №16**

**Тема:** Скомпрометований хост, ізольований за методикою 5 елементів

**Мета:** навчитися аналізувати журнали під час використання задокументованої уразливості для визначення скомпрометованих вузлів і файлів.

**Питання для обговорення:**

1. Підготовка віртуального середовища
2. Розвідувальна атака
3. Застосування експлоїтів
4. Проникнення

5. Перегляд журналів  
Література: 1, 2.

### 6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання вибраного наскрізного завдання. Орієнтовна тематика наскрізних завдань:

№ п/п	Тематика
1	Налаштування SOC
2	Дослідження безпеки кінцевих пристроїв.
3	Захист від шкідливого ПЗ на рівні хоста.
4	Захист від шкідливого ПЗ на рівні мережі.
5	Рішення для захисту від складного шкідливого програмного забезпечення Cisco AMP.
6	Міжмережеві екрани на рівні хоста.
7	Виявлення аномалій мережі
8	Перевірка мережі на уразливості
9	Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS).
10	База вразливостей CVE.
11	Розробка політики безпеки
12	Контроль вразливостей
13	Моніторинг безпеки
14	Реагування на інциденти і їх обробка
15	Структура правила Snort.
16	Робота в Sguil. Запити в Sguil.
17	Обробка подій в Sguil.
18	Реагування на інциденти і їх обробка
19	Життєвий цикл реагування на інциденти NIST.
20	Етапи виявлення та аналізу інцидентів.

### 7. Організація та проведення тренінгу з дисципліни з дисципліни «Кібернетична безпека»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Підготовка віртуального середовища	1. Запуск Oracle VirtualBox 2. Налаштування CyberOps Workstations 3. Запустіть віртуальні машини CyberOps Workstation, Kali, Metasploitable та Security Onion та увійдіть на них у систему
2	Розвідувальна атака	У цій частині ви будете використовувати nmap, щоб визначити, чи немає на віртуальній машині Metasploitable уразливостей, пов'язаних з програмою vsftpd
3	Застосування експлоїтів	Тепер, коли ви визначили, що можете отримати доступ з правами root на віртуальну машину Metasploitable, ви використовуватимете вразливість vsftp, щоб отримати повний контроль над віртуальною машиною Metasploitable. Ви компрометуватимете файл /etc/shadow і зможете отримати доступ до інших хостів в мережі.
4	Проникнення	1. Зламування паролів за допомогою утиліти John the Ripper 2. Пошук цільового вузла 3. Вилучення конфіденційного файлу

5	Перегляд журналів	1. Перегляньте оповіщення в Sguil 2. Перейдіть на Wireshark 3. Використовуйте ELSA для переходу до журналів Bro 4. Використовуйте ELSA для перегляду вибіраних даних
---	-------------------	---

### 8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проєктора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

### 9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Кібернетична безпека» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

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

### 10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Кібернетична безпека» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10 %	10 %	10 %	10 %	5 %	10 %	40 %
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-8.	Підсумкова письмова робота за темами №1-7.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 9-16.	Підсумкова письмова робота за темами №8-14	Визначається як середнє арифметичне з оцінок за виконання п'яти завдань тренінгу.	Оцінка за даний модуль виставляється за виконання вибраного наскрізного завдання.	1. 20 тестів по 3 бали - max 60 балів. 2. Практичне завдання - max 40 балів

### Шкала оцінювання:

За шкалою ЗУНУ	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)

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

№	Найменування	Номер теми
1.	Мультимедійний проектор	1 - 14
2.	Комп'ютерна лабораторія. Доступ до Інтернету. Курс мережевої академії Cisco CyberOps Associate	1 - 14
3.	Oracle VirtualBox, віртуальні машини: CyberOps, Security Onion, Kali Linux, Metasploitable; Cisco Packet Tracer 8.0, Ubuntu Server, OpenSSH, OpenVAS, Wireshark, Nmap, John the Ripper.	1 - 14

### РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Курс мережевої академії Cisco: CyberOps Associate. 2020. Режим доступу: <https://www.netacad.com/courses/cybersecurity/cyberops-associate>
1. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарев А. Видавництво Львівська політехніка, 2019. – 580.
2. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), № 45, ст.403 зі змінами від 28.07.2022 року. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
3. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective* 31. 4, 2022. – pp. 466-478.
4. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." *ACM Computing Surveys (CSUR)* 54.3, 2021. – pp.1-36
5. Santos, Henrique MD. *Cybersecurity: A Practical Engineering Approach*. CRC Press, 2022. – 341 p.
6. Grubb S. *How Cybersecurity Really Works*. 2021. – 219 p.
7. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
8. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
9. Cisar, P., & Pinter, R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, 9(4), 2019, pp.129-149.
10. Stallings, W. *Effective Cybersecurity: Understanding and Using Standards and Best Practices*. Addison-Wesley. 2019. – 893 p.
11. Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., & Vasquez, M. *The Official (ISC) 2 Guide to the CISSP CBK Reference*. John Wiley & Sons. 2019. – 928 с.