Чернівецький національний університет імені Юрія Федьковича

(повне найменування головного закладу вищої освіти)

Відокремлений структурний підрозділ «Фаховий коледж

Чернівецького національного університету імені Юрія Федьковича»

(повна назва відокремленого структурного підрозділу)

Циклова комісія *комп'ютерної інженерії*

(назва циклової комісії)

"**ПОГОДЖЕНО**"	"**ЗАТВЕРДЖУЮ**"
Завідувач	Заступник директора
Природничого відділення	з навчально-методичної роботи
_____ *В.В. Ковдриш*	_____ *М.Я. Дерев'янчук*
(підпис) (ініціали та прізвище)	(підпис) (ініціали та прізвище)
"___"_____20___року	"___"_____20___року

СИЛАБУС

навчальної дисципліни

"Основи кібербезпеки"

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

вибіркова

(вказати: обов'язкова/вибіркова)

Освітньо-професійна програма

"Прикладна математика"

(назва освітньо-професійної програми)

Спеціальність

113 "Прикладна математика"

(код і назва спеціальності)

Галузь знань

11 "Математика та статистика"

(код і назва галузі знань)

Освітньо-професійний ступінь

фаховий молодший бакалавр

(назва освітньо-професійного ступеня)

Мова навчання

українська

(вказати: на якій мові читається предмет)

Чернівці, 2020 рік

Силабус навчальної дисципліни *“Основи кібербезпеки”*

(назва навчальної дисципліни)

складений відповідно до освітньо-професійної програми

“Прикладна математика”

(назва освітньо-професійної програми)

затвердженої Вченою радою Чернівецького національного університету імені Юрія Федьковича (Протокол № *5* від «*25*» *травня* 20*20* року) та введеної в дію наказом ректора №*142* від «*27*» *травня* 20*20* року.

Розробники: (вказати авторів, їхні посади, наукові ступені та вчені (педагогічні) звання)

викладач, Х.В. Мельничук

викладач, О.В. Букурос

Профайл викладача (-ів)	http://college-chnu.cv.ua/article/5f896397d6f28212d7d8b03b
E-mail	h.melnychuk@chnu.edu.ua o.bukuros@chnu.edu.ua
Сторінка курсу в Moodle	
Консультації	понеділок з 15:00 до 16:00

Силабус навчальної дисципліни обговорено та узгоджено на засіданні циклової комісії

комп’ютерної інженерії

Протокол № ____ від “ _____” _____20___ року

Голова циклової комісії _____ *О.Ю. Тащук*

(підпис) (ініціали та прізвище)

Схвалено Методичною радою ВСП «Фаховий коледж ЧНУ імені Юрія Федьковича»

Протокол № ____ від “ _____” _____20___ року

Голова методичної ради _____ *О.Я. Білокрила*

(підпис) (ініціали та прізвище)

ПЕРЕЗАТВЕРДЖЕНО

Протокол № _____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № _____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № _____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

1. Загальні відомості про дисципліну

Анотація. Розвиток суспільства у XXI-му сторіччі не можна уявити без комп'ютерів, комп'ютерних мереж, Інтернету. У повсякденному спілкуванні слово Інтернет означає не лише глобальну мережу, яка об'єднує мільйони комп'ютерів і локальних мереж усього світу, а єдиний глобальний інформаційний простір – сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах.

За короткий проміжок часу Інтернет значно змінив наш спосіб життя, включаючи робочі процеси, способи навчання і розваг. Останнім часом до Інтернету здійснюється підключення не тільки комп'ютерів, а й всіляких фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації, які людина може використовувати в повсякденному житті.

Проте поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, в цей час активно поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Сучасні інформаційно-комунікаційні технології використовуватися навіть для вчинення терористичних актів.

Особливо безпечне користування Інтернетом стосується підростаючого покоління. Нині значна частина життя молоді «проходить» в Інтернеті, практично кожен студент має аккаунт в соціальній мережі, використовує Інтернет для навчання та розваг.

Кібербезпека – дуже важливий аспект освіти сучасного студента. Кожен здобувач освіти повинен володіти навичками грамотного поводження з інформацією, такі компетентності потрібно формувати одночасно з початковими навиками володіння персональним комп'ютером.

Кіберзагрози існують повсюди де застосовуються інформаційні технології, отже, студент будь-якої спеціальності, враховуючи умови сьогодення, в своїй діяльності стикається і зі спамом, і з вірусами, і зі зломом комп'ютера і з багатьма іншими проблемами, на які потрібно вміти не тільки оперативно реагувати, але і наскільки можливо вміти запобігати їх появі.

Курс «Основи кібербезпеки» спрямований на оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі; ознайомлення з різними типами зловмисного програмного забезпечення та атаками, а також методами захисту від них.

Мета. Метою вивчення навчальної дисципліни «Основи кібербезпеки» є формування у студентів теоретичної та практичної бази знань з безпечної поведінки в мережі; умінь і навичок ефективно та безпечно налаштовувати свої

облікові записи; розуміння принципів передачі даних через мережу та існуючих алгоритмів шифрування.

Завдання. Завдання курсу – навчитися безпечно поводитися в Інтернеті, налаштовувати безпеку систем і мереж, своїх облікових записів. Предмет курсу становлять використання основних засобів налаштувань політик безпеки системи, програмні додатки симуляції роботи мереж та налаштування їх безпеки, використання алгоритмів шифрування для закодування інформації.

Пререквізити. Дисципліна «Основи кібербезпеки» може вивчатись одночасно або після вивчення предмету «Інформатика», що підвищує ефективність засвоєння курсу.

Під час вивчення дисципліни «Основи кібербезпеки» студенту рекомендується пройти курси «Introduction to Cybersecurity» та «Cybersecurity Essentials» на сайті https://www.netacad.com.

У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:

знати:

- типові загрози, атаки та області їх розповсюдження;
- проблеми захисту даних;
- засоби протидії злочинності;
- основні поняття криптографії, алгоритми шифрування;
- поняття ідентифікації, методів аутентифікації, авторизації;
- основні типи засобів контролю цілісності даних;
- технології реагування на інциденти;
- основні кіберзакони, стандарти та відповідальність.

вміти:

- ідентифікувати можливі загрози чи атаки;
- налаштовувати локальну та групову політики безпеки системи;
- налаштовувати безпеку локальної мережі;
- шифрувати конфіденційні дані стандартними алгоритмами шифрування;
- налаштовувати безпеку веб-браузера;
- користуватися цифровим підписом;
- налаштовувати брандмауер;
- відрізняти та розуміти який метод шифрування найкраще підійде для використання в певних умовах;
- налаштовувати базову безпеку на маршрутизаторі;
- застосовувати знання з кібербезпеки в практичній діяльності.

2. Опис навчальної дисципліни

2.1. Загальна інформація

Назва навчальної дисципліни ***"Основи кібербезпеки"***						
Форма навчання	Рік підготовки	Семестр	Кількість			Вид підсумкового контролю
			Кредитів	Годин	Модулів	
Денна	2	3-4	3	90	3	**ЗАЛІК**

2.2. Дидактична карта навчальної дисципліни

№ за/п	Назви модулів і тем	Усього годин
МОДУЛЬ 1		
1	**Тема 1.** Потреба кібербезпеці	**2**
2	**Тема 2.** Атаки, поняття та методи	**4**
3	**Тема 3.** Захист даних та конфіденційність	**4**
4	**Тема 4.** Захист організації	**6**
Разом за модулем 1		**16**
МОДУЛЬ 2		
5	**Тема 5.** Кібербезпека – Світ експертів і злочинців	**4**
6	**Тема 6.** Куб кібербезпеки.	**6**
7	**Тема 7.** Загрози, вразливості та атаки	**8**
8	**Тема 8.** Мистецтво захисту таємниць	**10**
9	**Тема 9.** Мистецтво забезпечення цілісності	**10**
Разом за модулем 2		**38**
МОДУЛЬ 3		
10	**Тема 10.** Концепція «п'яти дев'яток»	**12**
11	**Тема 11.** Захист домену кібербезпеки	**16**
12	**Тема 12.** Спеціаліст з кібербезпеки	**8**
Разом за модулем 3		**36**
Усього за курс		**90**

2.2.1. Теми лекційних занять

№	Назва теми
1	**Тема 1.** Потреба кібербезпеці **План** **1.1.** Правові та етичні проблеми кібербезпеки **1.2.** Персональні дані **1.3.** Корпоративні дані **1.4.** Зловмисники та експерти з кібербезпеки **1.5.** Кібервійни
2	**Тема 2.** Атаки, поняття та методи **План** **2.1.** Аналіз кібератаки **2.2.** Ландшафт кібербезпеки
3	**Тема 3.** Захист даних та конфіденційність **План** **3.1.** Захист особистих даних **3.2.** Захист конфіденційності в інтернеті
4	**Тема 4.** Захист організації **План** **4.1.** Міжмережні екрани **4.2.** Підхід до кібербезпеки на основі поведінки **4.3.** Підхід Cisco до кібербезпеки
5	**Тема 5.** Кібербезпека – світ експертів і злочинців **План** **5.1.** Світ кібербезпеки **5.2.** Кіберзлочинці проти фахівців з безпеки **5.3.** Типові загрози **5.4.** Розповсюдження загроз кібербезпеки **5.5.** Підготовка більшої кількості спеціалістів
6	**Тема 6.** Куб кібербезпеки. **План** **6.1.** Три виміри куба кібербезпеки **6.2.** Тріада КЦД **6.3.** Стани даних **6.4.** Засоби протидії кіберзлочинності **6.5.** Структура керування ІТ безпекою
7	**Тема 7.** Загрози, вразливості та атаки **План** **7.1.** Шкідливе програмне забезпечення та зловмисний код **7.2.** Обман **7.3.** Атаки

8	**Тема 8.** Мистецтво захисту таємниць **План** **8.1.** Криптографія **8.2.** Контроль доступу **8.3.** Приховування даних
9	**Тема 9.** Мистецтво забезпечення цілісності **План** **9.1.** Типи засобів контролю цілісності даних **9.2.** Цифрові підписи **9.3.** Сертифікати **9.4.** Забезпечення цілісності баз даних
10	**Тема 10.** Концепція п’яти дев’яток **План** **10.1.** Висока доступність **10.2.** Заходи для поліпшення доступності **10.3.** Реагування на інциденти **10.4.** Відновлення після катастроф
11	**Тема 11.** Захист домену кібербезпеки **План** **11.1.** Захист систем та пристроїв **11.2.** Укріплення захисту серверів **11.3.** Укріплення захисту мережі **11.4.** Фізична безпека
12	**Тема 12.** Спеціаліст з кібербезпеки **План** **12.1.** Домени кібербезпеки **12.2.** Розуміння етики роботи у кібербезпеці **12.3.** Дослідження професії кібербезпеки

2.2.2. Теми лабораторних занять

№	Назва теми
МОДУЛЬ І	
1	Корпоративні дані. Порівняння даних за допомогою хешу.
2	Наслідки порушення безпеки. Що було зроблено?
3	Захист даних. Створення та збереження надійних паролів.
4	Обслуговування даних. Резервне копіювання даних до зовнішнього сховища.
5	Обслуговування даних. Резервне копіювання даних до зовнішнього сховища. Хто володіє вашими даними?
6	Захист конфіденційності в Інтернеті. Ризики поведінки в Інтернеті.
МОДУЛЬ ІІ	
7	Ідентифікація загроз
8	Packet Tracer. Створення кібер-світу
9	Packet Tracer. Комунікація у кіберсвіті
10	Встановлення віртуальної машини на персональному комп'ютері
11	Вивчення аутентифікації, авторизації та обліку
12	Packet Tracer. Вивчення шифрування файлів і даних
13	Packet Tracer. Використання перевірок цілісності файлів та даних
14	Виявлення загроз та вразливостей
15	Налаштування WEP/WPA2 PSK/WPA2 RADIUS
16	Використання стеганографії
17	Packet Tracer. Налаштування транспортного режиму VPN
18	Packet Tracer. Налаштування тунельного режиму VPN
19	Злам паролів. Використання цифрових паролів.
20	Віддалений доступ
МОДУЛЬ ІІІ	
21	Packet Tracer. Резервування маршрутизаторів і комутаторів
22	Packet Tracer. Стійкість маршрутизаторів і комутаторів
23	Захист Linux систем
24	Packet Tracer. Брандмауери на сервері та ACL на маршрутизаторі
25	Packet Tracer. Перевірка вмінь

2.2.3. Теми практичних завдань

№	Назва теми
МОДУЛЬ І	
1	Ідентифікація категорій вразливостей.
2	Визначення типів шкідливих програм.
3	Визначення типу атаки.
4	Визначення типу міжмережного екрану.
5	Визначення відповіді програми сканування портів.
6	Визначення пристрою безпеки.
7	Впорядкування етапів ланцюга кібервбивства (Kill Chain)
8	Визначення термінології за темою «Підхід до кібербезпеки»
МОДУЛЬ ІІ	
1	Вправа «Якого кольору мій капелюх»
2	Протидія кібер-злочинцям
3	Визначте спеціалізовані напрямки NIST/NICE з кібербезпеки
4	Визначення принципів інформаційної безпеки
5	Дані в обробці. Визначити стан даних
6	Політики та процедури кібербезпеки. Визначити категорію контрзаходів
7	Визначення галузей та елементів контролю ISO/IEC 27000
8	Визначити типи шкідливого ПЗ
9	Ідентифікувати атаки на браузер та електронну пошту
10	Ідентифікація тактики соціальної інженерії
11	Визначення загроз соціальної інженерії
12	Визначення типу кібератаки
13	Визначення типів атак на застосунки та веб-атак
14	Вивчення можливостей шифру Віженера
15	Інтерактивне завдання. Використання симетричного шифрування
16	Інтерактивне завдання. Використання асиметричного шифрування
17	Порівняння симетричного та асиметричного шифрування
18	Визначення стратегій розмежування доступу
19	Визначення методів аутентифікації
20	Порівняння засобів контролю безпеки
21	Визначити термінологію хешування
22	Порядок кроків в процесі цифрової сертифікації
23	Визначення засобів контролю цілісності бази даних
МОДУЛЬ ІІІ	
1	Заходи для поліпшення доступності. Виконання аналізу ризиків активів.
2	Заходи для поліпшення доступності. Визначити рівень захисту
3	Розташуйте у відповідному порядку етапи реакції на інциденти
4	Захист бездротових та мобільних пристроїв
5	Захист систем та пристроїв

6	Укріплення безпеки сервера
7	Підвищення рівня захисту мережі
8	Зіставлення доменів кібербезпеки
9	Дослідження кібер-етики
10	Зіставлення законів про кібербезпеку
11	Зброя кібербезпеки. Використання відповідних інструментів

2.2.4. Самостійна робота

№	Назва теми
1	DoS, DDoS та SEO
2	Надійна аутентифікація
3	Підхід Cisco до кібербезпеки
4	Області (домени) кібербезпеки. Сертифікація з кібербезпеки
5	Стани даних. Модель кібербезпеки ISO
6	Кібервійни
7	Приховування даних. VPN
8	Забезпечення цілісності БД. Цифрові сертифікати
9	Безпека на основі аналізу поведінки
10	Укріплення захисту серверів. Фізична безпека
11	Розуміння етики роботи у кібербезпеці.

3. Система контролю та оцінювання

3.1. Види та форми контролю

Формами поточного контролю є виконання лабораторних робіт, виконання вправ, тестування інструментом «Практика термінів та концепцій», усні відповіді студента, контрольні та підсумкові модульні контрольні роботи на платформі www.netacad.com та ін.

Формами підсумкового контролю є ЗАЛІК.

3.2. Засоби оцінювання:

Засобами оцінювання та демонстрування результатів навчання є:

- лабораторні роботи;
- вправи;
- практика термінів та концепцій;
- контрольні роботи;
- підсумкові модульні контрольні роботи;
- стандартизовані тести;
- студентські виступи на кіберзаходах.

3.3. Розподіл балів, що отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)															Кількість балів (залік)	Сумарна кількість балів
Модуль №1					Модуль № 2						Модуль № 3					
Т1	Т2	Т3	Т4	МКР	Т5	Т6	Т7	Т8	Т9	МКР	Т10	Т11	Т12	МКР	50	100
2	1	4	1	5	6	4	2	5	3	5	2	2	3	5		

3.4. Критерії оцінювання результатів навчання

У наведеній ниче таблиці вказано критерії, за якими визначається рівень навчальних досягнень студентів. Кожному балу відповідає певний відсоток правильних відповідей студентів на контрольних роботах. Слід вважати, що знання, уміння та навички студента відповідають певному рівню навчальних досягнень, якщо вони відповідають критерію, вказаному для цього рівня, та критеріям для всіх попередніх рівнів.

Рівні навчальних досягнень	Оцінка за шкалою ECTS	Критерії оцінювання навчальних досягнень студентів
І. Початковий	**F**	• розпізнає окремі об’єкти, явища і факти предметної галузі; • знає і виконує правила безпеки життєдіяльності під час роботи з комп’ютерною технікою. *Оцінка відповідає до 33,9% суми правильних відповідей*
	FX	• розпізнає окремі об’єкти, явища і факти предметної галузі та може фрагментарно відтворити знання про них. *Оцінка відповідає 33,9-48,9% суми правильних відповідей*
ІІ. Середній	**E**	• має фрагментарні знання незначного загального обсягу за відсутності сформованих умінь та навичок; • має елементарні навички роботи на комп’ютері; • виконує елементарне навчальне завдання із допомогою викладача. *Оцінка відповідає 50-58,9% суми правильних відповідей*
	D	• має початковий рівень знань, значну (більше половини) частину навчального матеріалу може відтворити; • може з допомогою викладача відтворити значну частину навчального матеріалу; • має стійкі навички виконання елементарних дій з опрацювання даних на комп'ютері. *Оцінка відповідає 65-69,9% суми правильних відповідей*
ІІІ. Достатній	**C**	• пояснює основні поняття навчального матеріалу; • може самостійно відтворити значну частину навчального матеріалу; • вміє застосовувати вивчений матеріал у стандартних ситуаціях; • має стійкі навички виконання основних дій з опрацювання даних на комп'ютері; • може пояснити основні процеси, що відбуваються під час роботи інформаційної системи, та наводити власні приклади на підтвердження деяких тверджень; • вміє виконувати навчальні завдання передбачені програмою. *Оцінка відповідає 70-78,9% суми правильних відповідей*
	B	• вміє аналізувати навчальний матеріал, в цілому самостійно застосовувати його на практиці; • вміє контролювати власну діяльність; • вміє систематизувати і узагальнювати отримані відомості; • може самостійно виправляти вказані викладачем помилки; • вміє самостійно визначати спосіб розв’язування навчальної задачі; • може аргументовано обрати раціональний спосіб виконання навчального завдання; • використовує електронні засоби для пошуку потрібної інформації. *Оцінка відповідає 80-88,9% суми правильних відповідей.*

IV. Високий	**A**	• Знання, вміння і навички учня відповідають вимогам програми у повному обсязі; • вміє планувати особисту навчальну діяльність, оцінювати результати власної практичної роботи; • володіє міцними знаннями, самостійно визначає проміжні етапи власної навчальної діяльності, аналізує нові факти, явища; • вміє самостійно знаходити додаткові відомості та використовує їх для реалізації поставлених перед ним навчальних завдань, судження його логічні і достатньо обґрунтовані; • використовує набуті знання і вміння у нестандартних ситуаціях; • вміє виконувати завдання, не передбачені навчальною програмою; • вміє самостійно знаходити джерела різноманітних відомостей і використовувати їх відповідно до мети і завдань власної пізнавальної діяльності; • вільно опановує та використовує нові інформаційно-комунікаційні технології для поповнення власних знань та розв'язування задач; • має сформовані стійкі навички керування інформаційними системами. *Оцінка відповідає 90-100,0% суми правильних відповідей.*

3.5. ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Сума балів за всі види навчальної діяльності	**Оцінка ЄКТС**	**Оцінка за національною шкалою**
90-100	**A**	зараховано
80-89	**B**	
70-79	**C**	
60-69	**D**	
50-59	**E**	
35-49	**FX**	не зараховано з можливістю повторного складання
0-34	**F**	не зараховано з обов'язковим повторним вивченням дисципліни

4. Перелік питань для підсумкового контролю (залік)

1. Правові та етичні проблеми кібербезпеки

2. Персональні дані як ціль.

3. Основні поняття «Корпоративних даних». Наслідки порушення безпеки.

4. Профіль кібер-зловмисника. Класифікація зловмисників.

5. Внутрішні та зовнішні загрози.

6. Основні поняття та мета кібервійни.

7. Історія комп'ютерних вірусів.

8. Вразливість системи безпеки та експлойти.

9. Типи вразливостей системи безпеки. Ідентифікація категорій вразливостей.

10. Типи зловмисного ПЗ та його симптоми. Визначення типів шкідливих програм.

11. Методи проникнення.

12. DoS, DDos та SEO. Визначення типу атаки.

13. Змішана атака. Зменшення наслідків атаки.

14. Захист пристроїв та мережі. Обслуговування даних.

15. Антивіруси – технології, індустрія, практичне застосування.

16. Загрози для мобільних пристроїв. Принципи безпечної роботи з мобільними пристроями.

17. Надійна аутентифікація. Поширення особистої інформації.

18. Типи міжмережних екранів.

19. Визначення відповіді програми сканування. Пристрої безпеки.

20. Виявлення атак у реальному часі.

21. Виявлення шкідливого програмного забезпечення.

22. Найкращі практики безпеки. Безпека електронних фінансів

23. Ботнет.

24. Ланцюг кібервбивства. Впорядування етапів ланцюга кібервбивства (KillChain)

25. Безпека на основі аналізу поведінки.

26. NetFlow і кібератаки.

27. Збірка сценаріїв з організації захисту.

28. Інструменти для запобігання та виявлення інцидентів. Системи IDS а IPS.

29. Області кібербезпеки

30. Кіберзлочинці та спеціалісти з кібербезпеки

31. Області розповсюдження загроз

32. Сертифікація з кібербезпеки

33. Конфіденційність

34. Доступність

35. Цілісність

36. Стани даних

37. Технології протидії кіберзлочинності

38. Політики та процедури кібербезпеки

39. Моделі кібербезпеки ISO та її використання

40. Типи шкідливого ПЗ

41. Атаки через браузер та електронну пошту

42. Методи обману

43. Типи кібератак

44. Атаки на бездротові мережі та мобільні пристрої

45. Атаки на застосунки

46. Основні поняття криптографії

47. Асиметричне шифрування

48. Симетричне шифрування

49. Типи контролю доступу

50. Ідентифікація, аутентифікація, авторизація

51. Приховування даних

52. Алгоритми хешування

53. Додавання солі, HMAC

54. Цифрові підписи

55. Цифрові сертифікати

56. Цілісність баз даних

57. П’ять дев’яток

58. Заходи для поліпшення доступності

59. Фази реагування на інциденти

60. Технології реагування на інциденти

61. Відновлення після катастроф

62. Укріплення хоста

63. Захист бездротових та мобільних пристроїв

64. Захист даних на хостах

65. Керування вмістом і образами

66. Фізичний захист робочих станцій

67. Укріплення захисту серверів

68. Укріплення захисту мережі

69. Фізична безпека

70. Домени кібербезпеки

71. Кібер закони та відповідальність

72. Етика та керівні принципи

5. Рекомендована література

5.1. Базова (основна)

1. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2010. - 508 с
2. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.
3. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, - К.; ПВП «Задруга», 2014. - 222 с
4. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
5. Навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.
6. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.
7. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p.
8. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978- 3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p.

5.2. Допоміжна

1. Лабораторний практикум з навчальної дисципліни "Інформаційна безпека". Навчально-практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 256 с. (Укр. мов.)
2. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб./ За заг. ред. Проф. Я.Ю. Кондратьєва. – К., 2004.
3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.
4. Методичні рекомендації для виконання лабораторних робіт з дисципліни АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ / [Ю. Є. Добришин, І.О.Чернозубкін]; Університет економіки та права «КРОК» – Київ - 2019. – 49 с.
5. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
6. К. Мандиа, К. Просис. Защита от вторжений. Расследование компьютерных преступлений. М., 2005.
7. Білоус Л. Ф. Інформаційні мережі : навч. посібник / Білоус Л. Ф. – К. : Логос, 2005. – 140 с.
8. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології : навчальний посібник / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. – Х. : "Компанія СМІТ", 2004. – 544 с
9. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем — К. : Видавнича група BHV, 2009. — 608 с.

10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22 https://tzi.ua/assets/files/%D0%9D%D0%94- %D0%A2%D0%97%D0%86-2.5-004-99.pdf
11. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12. 12. 2007 р. № 232. https://tzi.com.ua/downloads/3.1- 001-07.pdf

6. Інформаційні ресурси

1. https://www.netacad.com/
2. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
3. https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. https://zakon.rada.gov.ua/laws/show/3855-12#Text
5. https://zakon.rada.gov.ua/laws/show/2657-12#Text

Базою навчання є матеріали освітньої платформи CISCO NETWORKING ACADEMY

QR-код	Веб-посилання	Опис
	https://www.netacad.com/ru/courses/security/introduction-cybersecurity/	Мережева академія Cisco Networking Academy — це програма професійного і кар'єрного розвитку в сфері IT, яка доступна для навчальних закладів і студентів по всьому світу.