ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Основи інформаційної безпеки*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Петляк Наталія Сергіївна
Профайл викладач(ів)	https://kb.khmnu.edu.ua/petlyak-nataliya-sergiyivna/
E-mail викладача(ів)	npetlyak@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6845
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us02web.zoom.us/j/88595100831 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр І (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	1	1	5	150	51	17	34	-	-	99	-	-	+	-

Анотація дисципліни

Дисципліна викладається для студентів очної денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та репродуктивні, ігрові, модульно-розвивальні, застосування інформаційно-комп'ютерних технологій (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити: вихідна

Кореквізити: операційні системи та технології їх захисту; нормативно-правове забезпечення кібербезпеки; безпека вебресурсів.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни є формування термінологічного фундаменту, знань та розуміння предметної області; ознайомлення студентів із основними методами, принципами та алгоритмами захисту інформації в інформаційних системах.

Предметом дисципліни є основи забезпечення інформаційної та кібербезпеки .

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації”:

компетентності:

КЗ 01. Здатність застосовувати знання у практичних ситуаціях;

КФ 01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

КФ 04. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

КФ 05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

результати навчання:

РН 02. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 05. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень;

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах;

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

Студент, який успішно завершив вивчення дисципліни, повинен: виявляти загальні знання та розуміння предметної області та розуміння професії; мати базові знання та практичні навички з використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, в тому числі для забезпечення функціонування спеціального програмного забезпечення з захисту інформації від руйнуючих програмних впливів, а також для вирішення завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами і оцінки результативності якості прийнятих рішень; використовувати інформаційно-комунікаційних технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; вирішувати базові задачі управління процесами

відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Основи інформаційної безпеки** Загальні основи інформаційної безпеки	**ЛР1.** Кодування та шифрування даних як основа інформаційної безпеки	Опрацювання теоретичного матеріалу лекції №1.	6	[3] с.8-37 [7] с.8-27 [8] с.7-62
2	-	**ЛР1.** Підгрупа 2	Підготовка до виконання лабораторної роботи №1	6	[15]
3	**Тема 1. Основи інформаційної безпеки** Основні принципи кібербезпеки	**ЛР2.** Безпечне використання корпоративних систем обміну повідомленнями	Опрацювання теоретичного матеріалу лекції №2.	5	[1] с.83-85 [4] с.35-102
4	-	**ЛР2.** Підгрупа 2	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6	[30-31]
5	**Тема 1. Основи інформаційної безпеки** Безпечне використання корпоративних систем обміну повідомленнями	**ЛР3.** Організація та підтримка контролю цілісності даних та парольного доступу	Опрацювання теоретичного матеріалу лекції №3.	6	[9] с.500-547 [10] с.5-17 [11] с.1-9
6	-	**ЛР3.** Підгрупа 2	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6	[7] с.163-167 [8] [32]
7	**Тема 2. Архітектура комп'ютерів** Архітектура комп'ютерів	**ЛР4.** Встановлення віртуальних машин та операційних систем, інтеграція та оптимізація компонентів системи	Опрацювання теоретичного матеріалу лекції №4.	6	[1] с.146-148
8	-	**ЛР4.** Підгрупа 2	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6	[3] с.270-295 [26] [33]

9	**Тема 2. Архітектура комп'ютерів** Компоненти системи та робота з операційною системою	**ЛР5.** Захист від шкідливих програм, відновлення та резервування даних	Опрацювання теоретичного матеріалу лекції №5.	6	[12] с.8-35
10	-	**ЛР5.** Підгрупа 2	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	6	[6] с.106-121 [35-37]
11	**Тема 2. Архітектура комп'ютерів** Базові програми для забезпечення безпеки	**ЛР6.** Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів	Опрацювання теоретичного матеріалу лекції №6.	6	[1] с.316-343 [13] с.128-145, с.240-254
12	-	**ЛР6.** Підгрупа 2	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6	[3] с.105-159 [26] [40-41]
13	**Тема 3. Безпека мереж** Комп'ютерні мережі	**ЛР7.** Дослідження і налаштування інтегрованих засобів операційних систем для захисту даних	Опрацювання теоретичного матеріалу лекції №7.	6	[1] с.126-138 [5] с.106-127
14	-	**ЛР7.** Підгрупа 2	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6	[1] с.40-69, с.195-234 [42]
15	**Тема 4. Особливості застосування інформаційної безпеки** Основи безпеки даних в комп'ютерних системах	**ЛР8.** Безпечна робота із соціальними інтернет-сервісами та інструменти виявлення неправдивих повідомлень	Опрацювання теоретичного матеріалу лекції №8.	6	[6] с.76-102 [2] с.31-41
16	-	**ЛР8.** Підгрупа 2	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6	[43-46]

17	**Тема 4. Особливості застосування інформаційної безпеки** Забезпечення інформаційної безпеки у соціальних інтернет-сервісах	-	Опрацювання теоретичного матеріалу лекції №9.	4	[2] с.43-65, с.79-92 [14] с.1-11

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестовий контроль	Залік за рейтингом
Тема	1-4	1-4	
Ваговий коефіцієнт	0,6	0,4	

Оцінювання лабораторних занять. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і графічної частини; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Для виконання програми дисципліни студент повинен отримати 8 оцінок за лабораторні роботи.

Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її

на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку, отриману за лабораторну роботу, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	0-11	12-14	15–18	19-20
Оцінка за 4-ри бальною шкалою	2	3	4	5

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Вітчизняна оцінка, критерії**	
A	4,75–5,00	зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	незараховано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Способи подання інформації.
2. Основні характеристики інформації.
3. Основні принципи кібербезпеки.
4. Правила кібергігієни.
5. Корпоративні системи обміну повідомленнями (чати та інші) і відповідне програмне забезпечення.
6. Адміністрування корпоративних систем обміну повідомленнями
7. Системи числення.
8. Архітектура комп’ютерів.
9. Типи комп’ютерних архітектур.
10. Призначення ОС
11. Класифікація ОС
12. Архітектури ОС
13. Вразливості ОС
14. Будова комп'ютерних систем.
15. Комп'ютерні мережі.
16. Мережева модель OSI
17. Основні протоколи стеку TCP/IP
18. Зміст і основні поняття комп'ютерної безпеки
19. Основні поняття та стандарти інформаційної безпеки.
20. Класифікація загроз інформаційної безпеки.
21. Основні характеристики інформації.
22. Інформація як об’єкт посягань і захисту
23. Основні поняття щодо захисту інформації в автоматизованих системах.
24. Загрози безпеки даних та їх особливості.
25. Захист даних від комп'ютерних вірусів.
26. Шкідливі програми на ЕОМ.
27. Засоби захисту від комп'ютерних вірусів та їх особливості.
28. Вбудовані засоби операційних систем для захисту даних
29. Відновлення та резервування даних
30. Поняття соціальних інтернет-сервісів (СІС).
31. Вплив СІС на психіку користувачів.
32. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави.
33. Протидія впливу СІС.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
2. Кушнерьов. О.С. Безпека інформації : конспект лекцій – Суми : Сумський державний університет, 2021. – 99 с.
3. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020.– 236 с.
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
5. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
6. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. - Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
7. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інфомаційна та кібербезпека – К.: ДУТ, 2015. – 288 с.
8. Грабар І. Г., Грищук Р. В., Молодецька К. В.; за заг. ред. Грищука Р. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія – Житомир: ЖНАЕУ, 2019. – 280 с.
9. Бобало Ю. Я. та ін.; за заг. ред. д-ра техн. наук, проф. Бобала Ю. Я. та д-ра техн. наук, доц. Горбатого І. В. Інформаційна безпека: навч. посіб. - Львів: Видавництво Львівської політехніки, 2019. 580 с.
10. Бибка О.І. Конспект лекцій з дисципліни „Автоматизація адміністрування мережної інфраструктури" - Харків: ХНУРЕ, 2020. - 51с.
11. Архипова, Е., & Гудела, М. (2020). MODERN TRENDS IN THE FORMATION OF THE CORPORATE COMMUNICATION SYSTEM IN PUBLIC AUTHORITIES. SWorldJournal, 3(06-03), 75–83. https://doi.org/10.30888/2663-5712.2020-06-03-028
12. Федотова-Півень І. М., Миронець І. В., Півень О. Б., Сисоєнко С. В., Миронюк Т. В.; за ред. В. М. Рудницького. Операційні системи: навч.посіб. - Харків: ТОВ «ДІСА ПЛЮС»,2019. 216с.
13. Жаровський Р.О. Захист інформації у комп'ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
14. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). МЕТОДИКА ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(1), 6–16. https://doi.org/10.28925/2663-4023.2018.1.616
15. Олександр Мізюк. Системи числення. https://nrs.rozh2sch.org.ua/

Додаткова

16. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
17. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

18. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
19. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
20. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
21. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
22. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.
23. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ: ДП «УкрНДНЦ», 2018. – [50] с.
24. Барабаш О. В. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів / О. В. Барабаш, Р. В. Грищук, К. В. Молодецька-Гринчук // Наукоємні технології. – 2018. – № 2 (38). – С. 232–239. – Режим доступу: http://jrnl.nau.edu.ua/index.php/SBT/article/view/12855
25. Молодецька К. В. Механізми синергетично керованої самоорганізації акторів у соціальних інтернет-сервісах / К. В. Молодецька // Управління розвитком. – 2018. – Т. 4, вип. 4. – С. 1–13. – Режим доступу: http://ir.znau.edu.ua/handle/123456789/9582
26. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
27. Peter Dordal. An Introduction to Computer Networks / Peter Dordal, Loyola. – Independent, 2020. – 886c.
28. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ: Київ. нац. торг.-екон. ун-т, 2020. – 101 с.
29. Основні правила кібергігієни. Дата звернення 15.07.2023: https://cert.gov.ua/recommendation/31
30. Gursev Singh Kalra. "Threat analysis of an enterprise messaging system". [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1353485814701217#preview-section-abstract
31. Gerardus Blokdyk. (2019). Secure Messaging: A Complete Guide. Inc. ISBN: 0655820469. 480 p.
32. National Institute of Standards and Technology. (2017). An Introduction to Information Security. Special Publication 800-12r1. 101 p. Режим доступу : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
33. The Art of Service - Virtual Machines Publishing. (2021). Virtual Machines: A Complete Guide. Packt Publishing. ISBN: 186743556X. 500 p.
34. Захист від шкідливих програм і відновлення та резервування даних
35. Peter Dordal. An Introduction to Computer Networks / Peter Dordal, Loyola. – Independent, 2020. – 886c.
36. S. Gokulakrishnan and J. M. Gnanasekar, "Data integrity and recoverymanagement under peer-to-peer convoluted fault recognition cloud sys-tems," Journal of Computational and Theoretical Nanoscience, vol. 17,no. 5, pp. 2147–2150, 2020.
37. FreeVacy. (2023). Resources. [Електронний ресурс]. – Режим доступу : https://www.freevacy.com/resources
38. Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів
39. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
40. LazyAdmin, (2020) Home Network Security, [Електронний ресурс]. – Режим доступу : https://lazyadmin.nl/home-network/home-network-security

41. National Security Agency. (2022). Network Infrastructure Security Guide. [Електронний ресурс]. – Режим доступу : https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615
42. 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): 1-36.
43. Безпечна робота із соціальними інтернет сервісами та інструменти виявлення неправдивих повідомлень
44. Zhou, X., & Zafarani, R. (2020). A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. ACM Computing Surveys, 53(5), 1–40.
45. Social Engineering. [Електронний ресурс]. – Режим доступу : https://www.imperva.com/learn/application-security/social-engineering-attack/
46. Gardner, B. (2018). Social Engineering in Non-Linear Warfare. Journal of Applied Digital Evidence, 1(1). [Електронний ресурс]. – Режим доступу : http://mds.marshall.edu/jade/vol1/iss1/1

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php
3.