ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
підпис
_____ 20__ р.

СИЛАБУС

Навчальна дисципліна: **Основи інформаційної безпеки**

Освітньо-професійна програма: **Кібербезпека**

Рівень вищої освіти: **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Молодецька Катерина Валеріївна
Профайл викладача	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	kksmkhnu@gmail.com
Контактний телефон	Наявний в ІСУ
Сторінкадисциплінив ІСУ	https://msn.khnu.km.ua/course/view.php?id=5640
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/521227760 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2020-2021, семестр 1 (осінньо-зимовий)
Розклад занять	Лекції: середа, 4 пара (знаменник), онлайн Лабораторні роботи: підгрупа 1 – п'ятниця, 4-6 пара (чисельник), 4-502а підгрупа 2 – п'ятниця, 4-6 пара (знаменник), 4-502а
Консультації	Очні: понеділок, 1 пара, 1-103 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	Самостійнаробота, ут.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	1	6	180	68	17	51	-	-	112	-	-	+	-

Анотація дисципліни

Дисципліна „Основи інформаційної безпеки” - складова професійної підготовки бакалаврів зі спеціальності „Кібербезпека”, є однією зі спеціальних профілюючих дисциплін.

При викладанні дисципліни використовуються наступні форми (методи) навчання:пояснювально-ілюстративні, практичні, репродуктивні, ігрові, модульно-розвивальні, застосування інформаційно-комп’ютерних технологій (Virtual Box, R-Studio, інструменти та утиліти ОС Windows та Linux Ubuntu тощо), безпровідний маршрутизатор рівня SOHO Mercusys MW301R, підключення до мережі Internet.

Пререквізити: вихідна.

Кореквізити: стандарти і політики кібербезпеки, захищені бази даних

Мета і завдання дисципліни

Мета дисципліни. Формування термінологічного фундаменту, знань та розуміння предметної області. Ознайомлення студентів із основними методами, принципами та алгоритмами захисту інформації в комп’ютерних системах.

Предмет дисципліни. Основи забезпечення інформаційної та кібербезпеки.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії;

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

КФ 6. Здатність відновлювати штатне, функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;

результати навчання:

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 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-телекомунікаційні технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, Теорії та методи 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

Номер тижня	Номер теми	Тема лекції*	Тема лабораторного заняття**	Самостійна робота студента		
				Зміст	Години	Літера-тура
1	*2*	*3*	*4*	*5*	*6*	*7*
1	1		**ЛР1.** Кодування та шифрування даних як основа інформаційної безпеки	Опрацювання теоретичного матеріалу, підготовка до ЛР1	7	[8] с.763-837
2	1	Інформаційні технології як невід'ємна складова сучасного кіберсвіту	**ЛР1.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1	7	[3] с.78-320; [8] с.53-80, с.763-837
3	1		**ЛР2.** Встановлення віртуальних машин та операційних систем	Опрацювання теоретичного матеріалу, підготовка до ЛР2	8	[3] с.270-295
4	1	Загальні основи інформаційної безпеки	**ЛР2.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	7	[1] с.8-37; [5] с.8-27; [7] с.7-62 [3] с.270-295
5	1		**ЛР3.** Автентифікація, авторизація та облік користувачів в комп'ютерних системах	Опрацювання теоретичного матеріалу, підготовка до ЛР3	7	[6] с.176-189
6	1	Несанкціоноване зняття інформації Методи та засоби блокування технічних каналів витоку інформації	**ЛР3.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3	7	[6] с.20-33, с.176-189; [7] с.151-188
7	1		**ЛР4.** Організація та підтримка контролю цілісності даних та парольного доступу	Опрацювання теоретичного матеріалу, підготовка до ЛР4	6	[7] с.163-167
8	1	Основи безпеки даних в комп'ютерних системах	**ЛР4.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР4	6	[7] с.163-167 [6] с.5-19; [15] с.24-33, с.43-57
9	2		**ЛР5.** Відновлення та резервування даних	Опрацювання теоретичного матеріалу, підготовка до ЛР5	7	[6] с.106-121
10	2	Ідентифікація і аутентифікація користувачів	**ЛР5.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5	7	[6] с.106-121, с.176-189; [15] с.63-70

11	2		**ЛР6.** Хешування даних і використання цифрового підпису та стеганографії	Опрацювання теоретичного матеріалу, підготовка до ЛР6	7	[15] с.71-102
12	2	Основи захисту даних	**ЛР6.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	7	[7] с.154-188; [11] с.53-84; [15] с.71-102
13	2		**ЛР7.** Дослідження і налаштування інтегрованих засобів операційних систем для захисту даних	Опрацювання теоретичного матеріалу, підготовка до ЛР7	6	[1] с.40-69, с.195-234
14	2	Основи криптографії	**ЛР7.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	6	[1] с.40-69, с.141-193, с.195-234 ; [15] с.71-102
15	2		**ЛР8.** Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів	Опрацювання теоретичного матеріалу, підготовка до ЛР8	6	[3] с.105-159
16	2	Забезпечення інформаційної безпеки у соціальних інтернет-сервісах	**ЛР8.** (підгрупа 2)	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8	6	[3] с.105-159; [9] с.7-89, [15] с.34-43
17	2		Підсумкове заняття Тестування	Опрацювання теоретичного матеріалу, підготовка до тестового контролю	7	

* лекції проводяться раз на два тижні по 2 години;

** лабораторні проводяться по 6 годин раз на два тижні.

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.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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 заняття	Тестовий контроль	Залік за рейтингом
Тема	1-2	1-2	
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.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1-11	12-14	15–18	19-20
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 20 хвилин. Тестування проводиться з використанням

модульного середовища для навчання MOODLE. Правильні відповіді студент реєструє в он-лайн режимі в модульному середовищі MOODLE. Через 20 хвилин студенти завершують тестування та надсилають свої відповіді на сервер. Викладач оголошує результати тестування згідно журналу оцінок модульного середовища MOODLE.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
1	*2*
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.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає

набраній студентом кількості балів.

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

Питання для самоконтролю студентів

1. Способи подання інформації.
2. Системи числення.
3. Будова комп'ютерних систем (апаратні та програмні засоби).
4. Комп'ютерні мережі.
5. Зміст і основні поняття комп'ютерної безпеки
6. Основні поняття та стандарти інформаційної безпеки.
7. Класифікація загроз інформаційної безпеки.
8. Основні характеристики інформації.
9. Інформація як об’єкт посягань і захисту
10. Поняття технічних каналів витоку інформації та їх утворення.
11. Види та класифікація технічних каналів витоку інформації
12. Способи несанкціонованого зняття інформації.
13. Пасивний та активний захист інформації.
14. Захист акустичної інформації.
15. Захист електромагнітної інформації
16. Організаційні та технічні заходи захисту інформації.
17. Основні поняття щодо захисту інформації в автоматизованих системах.
18. Загрози безпеки даних та їх особливості.
19. Канали проникнення та принципи побудови систем захисту.
20. Основи фізичного захисту об'єктів.
21. Поняття про ідентифікацію користувача та її особливості.
22. Основні принципи та методи аутентифікації.
23. Захист даних від несанкціонованого доступу (НСД).
24. Основні принципи захисту даних від НСД.
25. Моделі управління доступом.
26. Технічні можливості зловмисника і засоби знімання інформації.
27. Технічні засоби захисту даних від їх витоку.
28. Захист даних від комп'ютерних вірусів.
29. Шкідливі програми на ЕОМ.
30. Засоби захисту від комп'ютерних вірусів та їх особливості.
31. Вбудовані засоби операційних систем для захисту даних
32. відновлення та резервування даних
33. Основи криптографії. Основні терміни та поняття.
34. Криптографічні методи захисту інформації.
35. Класичні техніки шифрування.
36. Симетричні та асиметричні алгоритми шифрування інформації.
37. Цифрові підписи.
38. Поняття соціальних інтернет-сервісів (СІС).
39. Вплив СІС на психіку користувачів.
40. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави.
41. 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

№	Назва	Режим доступу
1.	Козюра В.Д. Захист інформації в комп'ютерних системах: підручник. / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.	http://ir.stu.cn.ua/bitstream/handle/123456789/19248/3ахист%20інформ.%20в%20комп.%20сис.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
2.	Нестеров С.А. Основы информационной безопасности: Учебное пособие. / 3-е изд., стер. – СПб, Издательство "Лань", 2017. – 324с.	https://e.lanbook.com/reader/book/90153/#1 http://www.unibytes.com/lG1-y-jmQXMLqw-Us4P3UgBB
3.	Вишнівський В.В. Методи та засоби комп'ютерних ІТ. Навчальний посібник. / Вишнівський В.В., Гніденко М.П., Гайдур Г.І., Сєрих С.О. – Київ. – 2018. – 519 с.	http://www.dut.edu.ua/uploads/l_1683_92156142.pdf
4.	Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.	https://www.academia.edu/42885659/Fundamentals_Of_Information_Systems_Security_by_David_Kim_Michael_G_Solomon
5.	Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД "Гельветика", 2017. – 168 с.	http://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf
6.	Бондарев В.В.. Введение в информационную безопасность автоматизированных систем. – М.: ГТУ им. Н.Э. Баумана, 2016. – 252 с.	https://only-soft.org/viewtopic.php?t=84625
7.	Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.	http://www.dut.edu.ua/uploads/p_303_79299367.pdf
8.	Peter Dordal. An Introduction to Computer Networks / Peter Dordal, Loyola. – Independent, 2020. – 886с.	http://intronetworks.cs.luc.edu/current1/ComputerNetworks.pdf
9.	Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька ; за заг. ред. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с. - Режим доступу: http://ir.znau.edu.ua/handle/123456789/9581	http://ir.znau.edu.ua/handle/123456789/9581
10.	Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.	http://elartu.tntu.edu.ua/bitstream/123456789/18299/1/КБІМС%28посібник%29.docx
11.	Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ "ОЮА", 2017. – 128 с.	http://dspace.onua.edu.ua/bitstream/handle/11300/11111/ОІБ%20конспект%20лекцій.pdf?sequence=1&isAllowed=y
12.	Гур'єв В.І. Інформаційна безпека держави: навчальний посібник / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин:	http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.

	ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.	%20New%20booklet%201.pdf?sequence=1&isAllowed=y
13.	Бобало Ю.Я. Інформаційна безпека: 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; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing
14.	Соколов В.Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. – 2 вид., доп. - К. : КУБГ, 2019. – 130 с.	https://zenodo.org/record/2671768#.YAaeGHb7TIU http://elibrary.kubg.edu.ua/id/eprint/27294/1/V_Sokolov_V_Buriachok_M_Taj_Dini_WMS_2.pdf
15.	Пількевич І.А. Захист інформації в автоматизованих системах управління: навч. посібник / І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.	http://ir.znau.edu.ua/bitstream/123456789/3073/1/Zahyst_informacii_ASU.PDF

Додаткова

№	Назва	Режим доступу
16.	Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.	https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text
17.	ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.	https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
18.	ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.	https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
19.	ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.	http://ksv.do.am/GOST/DSTY_ALL/DSTU1/dstu_3396.2-97.pdf
20.	НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.	https://tzi.com.ua/downloads/1.1-002-99.pdf
21.	НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.	https://tzi.com.ua/downloads/1.4-001-2000.pdf
22.	Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.	https://zakon.rada.gov.ua/laws/show/2594-15#Text
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.	https://metrology.com.ua/?smd_process_download=1&download_id=8877
24.	Грищук Р. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. В. Грищук, К. В. Молодецька-Гринчук // Захист інформації. – 2017. – Т. 19, № 4. – С. 254–262.	http://jrnl.nau.edu.ua/index.php/ZI/article/download/12204/16442

25.	Hryshchuk R. Modelling of conflict interaction of virtual communities in social networking services on an example of anti-vaccination movement / R. Hryshchuk, K. Molodetska, Yu. Tymonin // Conflict Management in Global Information Networks : Proc. of the International Workshop on CMiGIN 2019. – 2019. – Vol-2588. – PP. 250–264.	http://ceur-ws.org/Vol-2588/paper21.pdf
26.	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.	http://jrnl.nau.edu.ua/index.php/SBT/article/view/12855
27.	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.	http://ir.znau.edu.ua/handle/123456789/9582
28.	Молодецька-Гринчук К. В. Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Вісник ЖНАЕУ. – 2017. – № 2 (61), т. 1. – С/ 180-187.	http://ir.znau.edu.ua/bitstream/123456789/8734/1/VZNAEU_2017_2_180-187.pdf
29.	Грищук Р. В. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблогу Twitter) / Р. В. Грищук, В. М. Мамарєв, К. В. Молодецька-Гринчук // Інформаційні технології та комп'ютерна інженерія. – 2017. – № 2. – с. 12-19, – Режим доступу: https://itce.vntu.edu.ua/index.php/itce/article/view/672	https://itce.vntu.edu.ua/index.php/itce/article/view/672
30.	Молодецька-Гринчук К. В. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня / К. В. Молодецька-Гринчук // Системи обробки інформації. - 2017. - Вип. 5. - С. 122-129.	http://nbuv.gov.ua/UJRN/soi_2017_5_18
31.	Грищук Р. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р.В. Грищук, К.В. Молодецька-Гринчук // Сучасний захист інформації. – 2018. – №1(33). – С. 43-52.	http://journals.dut.edu.ua/index.php/dataprotect/article/view/1793
32.	Молодецька-Гринчук К. В. Модель системи підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня / Катерина Валеріївна Молодецька-Гринчук // Безпека інформації, Ukrainian Scientific Journal of Information Security. – 2017. – Vol. 23, Issue 2. – P. 136-144.	http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/11803
33.	Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах / К. Молодецька-Гринчук // Автоматизація технологічних і бізнес-процесів. – 2017. – Volume 9, Issue 2. – С. 36-42	https://journals.onaft.edu.ua/index.php/atbp/article/view/560
34.	Молодецька-Гринчук К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 2 (26). – С. 104–110.	http://ir.znau.edu.ua/handle/123456789/7868
35.	Молодецька-Гринчук К. В. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності / К. В. Молодецька-Гринчук // Управління розвитком складних систем : зб. наук. праць / Київ. нац. ун-т буд-ва і архітектури ; гол. ред. П. П. Лізунов. – Київ : КНУБА, 2017. – № 30. – С. 121 - 127.	http://repositary.knuba.edu.ua:8080/xmlui/handle/987654321/4542

36.	Молодецька-Гринчук К. В. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2016. – № 4 (24). – С. 80–92.	http://ir.znau.edu.ua/handle/123456789/7870
37.	Молодецька К. В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. В. Молодецька // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84–93.	http://ir.znau.edu.ua/handle/123456789/7866
38.	Молодецька-Гринчук К. В. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками / К. В. Молодецька-Гринчук // Радіоелектроніка, інформатика, управління. - 2017. - № 2. - С. 117-126.	http://nbuv.gov.ua/UJRN/riu_2017_2_15
39.	Молодецька К. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К. Молодецька // Інформаційні технології та безпека. – 2016. – Vol. 4, № 1. – С. 13–20.	http://nbuv.gov.ua/UJRN/inftech_2016_4_1_4
40.	Грищук Р. В. Спосіб синергетичного управління поведінкою акторів у соціальних інтернет-сервісах / Р. В. Грищук, К. В. Молодецька // Системи управління, навігації та зв'язку. – 2016. – Вип. 1 (37). – С. 66–70.	http://ir.znau.edu.ua/handle/123456789/6278

Інформаційні ресурси

1. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khnu.km.ua.

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ (Підпис) д.т.н., професор (Вчений ступінь, звання) К.В. Молодецька (Ініціали, прізвище)

Погоджено
Гарант освітньої програми _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище)

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Ю.П. Кльоц (Ініціали, прізвище)