ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

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

СИЛАБУС

Навчальна дисципліна: “ *Побудова захищених комп'ютерних систем* ”

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Чешун Віктор Миколайович Анікін Володимир Андрійович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/cheshun-viktor-mykolajovych/ https://kb.khmnu.edu.ua/anikin-volodymyr-andrijovych/
E-mail викладача(ів)	cheshunvn@khmnu.edu.ua anikin_volodymyr@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=9069
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр IV (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
ОД	-	-	8	240	90	36	54			150			+	

Анотація дисципліни

Дисципліна «Побудова захищених комп'ютерних систем» є вибірковою, викладається для студентів очної денної форми навчання, рекомендована для здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня. При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити – немає.

Кореквізити – немає.

Мета і завдання дисципліни

Мета дисципліни. Формування у студентів системи знань про методи і засоби побудови захищених комп'ютерних систем з набуттям здатності застосовувати знання у практичних ситуаціях, виконувати пошук, оброблення та аналіз інформації і застосовувати нормативну документацію, державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Предмет дисципліни. Методи і засоби вимірювання електричних і неелектричних величин; Державна метрологічна служба України і міжнародні метрологічні організації; системи стандартизації і сертифікації України, ЄС та світу.

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

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.

результати навчання:

РН 1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки.

РН 8. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

Після вивчення дисципліни „Побудова захищених комп'ютерних систем” студент має:

знати:

- методи і засоби забезпечення єдності вимірювань;
- призначення та основні характеристики вимірювальних пристроїв;
- організацію, структуру та основні положення національної і міжнародної систем стандартизації із стандартизацією в галузі інформаційної безпеки включно;
- принципи впровадження стандартів та державного нагляду за їх дотриманням;
- загальні принципи сертифікації продукції, послуг, персоналу, систем управління (в тому числі в галузі інформаційної і кібербезпеки);
- вимоги державних стандартів України щодо оформлення текстової, програмної і графічної документації.

Студент, який успішно завершив вивчення дисципліни, повинен: *вміти* застосовувати методи вимірювання та оцінювати точність (похибки) вимірювань; користуватися спеціальною, довідковою та методичною літературою; використовувати нормативно-технічні документи і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки; розробляти і оформлювати супровідну текстову, програмну, конструкторську документацію технічного об’єкта у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо). *бути здатним*: обрати засоби вимірювань заданих величин, метод вимірювань і певну методику оцінки похибки виконаних вимірювань; використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел (державних та міжнародних стандартів й інших нормативних документів тощо) для ефективного рішення спеціалізованих задач професійної діяльності; оформити технічну документацію в процесі навчання (звіти, реферати, курсові проекти та кваліфікаційну роботу тощо) і професійної діяльності (інструкції, звіти, нормативні документи, політики безпеки тощо) у відповідності до вимог державних стандартів України (Єдиної системи конструкторської документації і Єдиної системи програмної документації тощо).

Тематичний і календарний план вивчення дисципліни

Номер тижня	Тема лекції*	Тема лабораторної роботи**	Самостійна робота студента		
			Зміст	Години	Літера-тура
1	*3*	*4*	*5*	*6*	*7*
1	**Введення в дисципліну** Взаємозв'язок метрологія-стандартизація-сертифікація. Метрологія: основні поняття та визначення. Види фізичних величин. Міжнародна система одиниць. Основні одиниці системи СІ. Похідні та позасистемні одиниці системи СІ. Кратні та частинні одиниці системи СІ.	Елементарні вимірювання неелектричних величин. Точність і похибки вимірювань.	Опрацювання теоретичного матеріалу, підготовка до ЛР 1	15	[2] с.25-52; [3] с.6-55; [4] с.120-123; [7] с.8-22; [8] с.7-46
2	**Вимірювальні засоби і прилади як інструмент метрології** Призначення і загальна класифікація вимірювальних засобів. Класифікація електронних вимірювальних приладів. Групи, підгрупи і шифри типів електронних вимірювальних приладів. Характеристики вимірювальних приладів. Вимоги до сучасних вимірювальних приладів.	Ознайомлення з вимірювальним обладнанням лабораторії	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 1, підготовка до ЛР 2	17	[3] с.110-122; [4] с.127-130; [6] с.28-30, 53-90; [7] с.32-42, 53-100, 125-157; [8] с.47-88, 186-252
3	**Методи, точність і похибки вимірювань** Вимірювання як метрологічний процес. Стандартизовані визначення характеристик вимірювань. Методи вимірювань. Фактори, що впливають на точність вимірювань. Похибки – поняття та класифікація.	Дослідження параметрів вимірювальних генераторів та частотомірів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 2, підготовка до ЛР 3	17	[2] с.55-66; [3] с.55-110; [4] с.123-127, 130-136; [6] с.13-27, 33-49; [8] с.89-119
4	**Нормативно-правова і організаційна база метрології** Нормативно-правова база метрології. Державна метрологічна система України. Міжнародні метрологічні організації. Система забезпечення єдності вимірювань.	Дослідження вимірювальних можливостей універсальних осцилографів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 3, підготовка до ЛР 4	17	[2] с.66-87; [3] с.155-200; [4] с.138-155; [7] с.23-31

5	**Стандартизація – основні поняття, задачі, методи, органи** Поняття, задачі, рівні стандартизації Нормативні документи державної стандартизації Органи державної стандартизації України Органи міжнародної стандартизації Система стандартизації країн ЄС.	Робота з мультиметром, вольтметром і амперметром. Вимірювання параметрів сигналів і компонентів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 4, підготовка до ЛР 5	17	[2] с.88-147; [3] с.200-224; [4] с.7-51
6	**Єдина система конструкторської документації (ЄСКД) – введення. Оформлення текстової документації за ЄСКД.** Єдина система конструкторської документації (ЄСКД) - основні поняття, визначення та призначення (ДСТУ ГОСТ 2.001:2006). Сфера поширення стандартів ЄСКД. Склад, класифікація й позначення стандартів ЄСКД. Види конструкторських документів (ДСТУ 3321:2003). Комплектність конструкторських документів. Загальні правила оформлення графічних і текстових документів. Основні надписи конструкторських документів. Етапи розробки конструкторської документації. Загальні вимоги до текстових документів (ГОСТ 2.105-95). Оформлення пояснювальної записки. Порядок викладення тексту документів. Правила написання позначень і найменувань одиниць фізичних величин. Оформлення ілюстрацій і додатків. Побудова таблиць. Оформлення списку літератури. Оформлення специфікації.	Побудова структурних і функціональних схем електронних пристроїв і систем у відповідності до вимог державних стандартів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 5, підготовка до ЛР 6	17	[14] ; [17] с.101-106; [20]; [21]
7	**Єдина система програмної документації (ЄСПД). Оформлення графічної документації і схем за ЄСКД та ЄСПД.** Єдина система програмної документації. Види графічних документів за ЄСКД. Правила нанесення розмірів. Загальні вимоги до робочих креслень.	Розробка схем електричних принципових у відповідності до вимог державних стандартів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 6, підготовка до ЛР 7	17	[14] ; [17] с.101-106; [20]; [21] ; [22]

	Креслення деталі. Креслення складальні. Креслення загального виду. Різновиди схем і загальні вимоги до їх виконання. Схеми електричні структурні. Схеми електричні функціональні. Схеми електричні принципові. Схеми з'єднань.				
8	**Стандартизація в галузі інформаційної і кібербезпеки** Початок стандартизації в інформаційній безпеці. Критерії безпеки комп'ютерних систем міністерства оборони США TCSEC. Розвиток стандартів інформаційної і кібербезпеки Міжнародні стандарти для системи управління інформаційною безпекою ISO 270xx.	Оформлення супровідної документації до схем електричних вузлів у відповідності до вимог державних стандартів	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 7, підготовка до ЛР 8	17	[11] с.28-50; [12] с.81-92; [13] с.148-170; [28] с.91-108
9	**Сертифікація – основні поняття, завдання, методи, органи. Сертифікація в інформаційній і кібербезпеці** Сертифікація – основні поняття і визначення. Види сертифікації. Загальні принципи сертифікації. Система сертифікації. Норми і правила сертифікації. Акредитація органів сертифікації. Сертифікація систем управління інформаційною безпекою. Міжнародна сертифікація фахівців в галузі інформаційної і кібербезпеки.	Підсумкове заняття, тестування	Опрацювання теоретичного матеріалу, підготовка до захисту звіту ЛР 8, підготовка до тестування	16	[2] с.233-302; [3] с.224-262; [4] с.51-116 ; [9] с.110-149

* лекції проводяться щотижня по 4 години; ** лабораторні роботи щотижня по 6 годин.

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 роботи згідно з розкладом, не запізнюватися на заняття, домашні завдання виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.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.

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

Аудиторна робота			**Контрольні заходи**	**Підсумковий контрольний захід**
Лабораторні роботи №:		Тестовий контроль 1	Тестовий контроль 2	Семестровий контроль
1 - 8		Т 1-3	Т 4-7	Залік
ВК:	0,8	0,2	0,2	

Оцінювання лабораторних робіт. 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 звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або 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 за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на

кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал 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.

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.

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 ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Взаємозв’язок метрологія-стандартизація-сертифікація.
2. Метрологія: основні поняття та визначення.
3. Види фізичних величин.
4. Міжнародна система одиниць.
5. Основні одиниці системи СІ.
6. Похідні та позасистемні одиниці системи СІ.
7. Кратні та частинні одиниці системи СІ.
8. Призначення і загальна класифікація вимірювальних засобів.
9. Класифікація електронних вимірювальних приладів.
10. Групи, підгрупи і шифри типів електронних вимірювальних приладів.
11. Характеристики вимірювальних приладів.
12. Вимоги до сучасних вимірювальних приладів.
13. Вимірювання як метрологічний процес.
14. Стандартизовані визначення характеристик вимірювань.
15. Методи вимірювань.
16. Фактори, що впливають на точність вимірювань.
17. Похибки – поняття та класифікація.
18. Нормативно-правова база метрології.
19. Державна метрологічна система України.
20. Міжнародні метрологічні організації.
21. Система забезпечення єдності вимірювань.
22. Поняття, задачі, рівні стандартизації
23. Нормативні документи державної стандартизації
24. Органи державної стандартизації України
25. Органи міжнародної стандартизації
26. Система стандартизації країн ЄС
27. Єдина система конструкторської документації (ЄСКД) - основні поняття, визначення та призначення (ДСТУ ГОСТ 2.001:2006).
28. Сфера поширення стандартів ЄСКД.
29. Склад, класифікація й позначення стандартів ЄСКД.
30. Види конструкторських документів (ДСТУ 3321:2003).
31. Комплектність конструкторських документів.
32. Загальні правила оформлення графічних і текстових документів за ЄСКД.
33. Основні надписи конструкторських документів за ЄСКД.
34. Етапи розробки конструкторської документації за ЄСКД.
35. Загальні вимоги до текстових документів (ГОСТ 2.105-95).
36. Оформлення пояснювальної записки за ЄСКД.
37. Порядок викладення тексту документів за ЄСКД.
38. Правила написання позначень і найменувань одиниць фізичних величин за ЄСКД.
39. Оформлення ілюстрацій і додатків за ЄСКД.
40. Побудова таблиць за ЄСКД.
41. Оформлення списку літератури за ЄСКД.
42. Оформлення специфікації за ЄСКД.
43. Єдина система програмної документації (ЄСПД).
44. Види графічних документів за ЄСКД.
45. Правила нанесення розмірів за ЄСКД.
46. Загальні вимоги до робочих креслень за ЄСКД.
47. Креслення деталі за ЄСКД.
48. Креслення складальні за ЄСКД.
49. Креслення загального виду за ЄСКД.
50. Різновиди схем і загальні вимоги до їх виконання за ЄСКД.
51. Схеми електричні структурні за ЄСКД.

52. Схеми електричні функціональні за ЄСКД.
53. Схеми електричні принципові за ЄСКД.
54. Схеми з'єднань за ЄСКД.
55. Початок стандартизації в інформаційній безпеці.
56. Критерії безпеки комп'ютерних систем міністерства оборони США TCSEC – базові положення.
57. Розвиток стандартів інформаційної і кібербезпеки – характерні тенденції.
58. Міжнародні стандарти для системи управління інформаційною безпекою ISO 270xx – роль в стандартизації питань інформаційної і кібербезпеки.
59. Стандарт ISO 27001 – роль і призначення.
60. Сертифікація – основні поняття і визначення.
61. Види сертифікації.
62. Загальні принципи сертифікації.
63. Система сертифікації.
64. Норми і правила сертифікації.
65. Акредитація органів сертифікації.
66. Сертифікація систем управління інформаційною безпекою.
67. Міжнародна сертифікація фахівців в галузі інформаційної безпеки.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Побудова захищених комп'ютерних систем” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. 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.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
3. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
4. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інфомаційна та кібербезпека. К.: ДУТ, 2015. 288 с.
5. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир: ЖНАЕУ, 2019. 280 с.
6. Інформаційна безпека: навч. посіб./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. Львів: В-во Львівської політехніки, 2019. 580 с.
7. Бибка О.І. Конспект лекцій з дисципліни „Автоматизація адміністрування мережної інфраструктури”. Харків: ХНУРЕ, 2020. 51с.
8. Архипова, Е., & Гудела, М. Modern trends in the formation of the corporate communication system in public authorities. SWorldJournal. 2020. №3(06-03), P. 75–83. URL: https://doi.org/10.30888/2663-5712.2020-06-03-028
9. 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.
10. Жаровський Р.О. Захист інформації у комп’ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
11. Sokolov V. Y., Kurbanmuradov, D. M. Методика протидії соціальному інжинірингу на об’єктах інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2018. №1(1). С. 6–16. https://doi.org/10.28925/2663-4023.2018.1.616
12. Олександр Мізюк. Системи числення. URL: https://nrs.rozh2sch.org.ua/

Додаткова

13. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
14. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
15. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
16. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
17. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
19. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.
20. 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.
21. Барабаш О. В., Грищук Р. В., Молодецька-Гринчук К. В. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів.Наукоємні технології.

2018. № 2 (38). С. 232–239. URL: http://jrnl.nau.edu.ua/index.php/SBT/article/view/12855

22. Молодецька К. В. Механізми синергетично керованої самоорганізації акторів у соціальних інтернет-сервісах. Управління розвитком. 2018. Т. 4, вип. 4. С. 1–13. Режим доступу: http://ir.znau.edu.ua/handle/123456789/9582

23. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. Third edition. Burlington :Jones & Bartlett Learning, 2018. 571 p.

24. Peter Dordal, Loyola. An Introduction to Computer Networks. Independent, 2020. 886c.

25. 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.

26. Основні правила кібергігієни. URL: https://cert.gov.ua/recommendation/31 Дата звернення 15.07.2023:

27. Gursev Singh Kalra. "Threat analysis of an enterprise messaging system". URL: https://www.sciencedirect.com/science/article/abs/pii/S1353485814701217#preview-section-abstract

28. Gerardus Blokdyk. (2019). Secure Messaging: A Complete Guide. Inc. ISBN: 0655820469. 480 p.

29. 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

30. The Art of Service - Virtual Machines Publishing. (2021). Virtual Machines: A Complete Guide. Packt Publishing. ISBN: 186743556X. 500 p.

31. Захист від шкідливих програм і відновлення та резервування даних

32. Peter Dordal. An Introduction to Computer Networks. Loyola. Independent, 2020. 886c.

33. 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.

34. FreeVacy. (2023). Resources. URL: https://www.freevacy.com/resources

35. Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів

36. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.

37. LazyAdmin, (2020) Home Network Security. URL: https://lazyadmin.nl/home-network/home-network-security

38. National Security Agency. (2022). Network Infrastructure Security Guide. URL: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615

39. 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.

40. Безпечна робота із соціальними інтернет сервісами та інструменти виявлення неправдивих повідомлень

41. Zhou, X., & Zafarani, R. (2020). A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. ACM Computing Surveys, 53(5), 1–40.

42. Social Engineering. URL: https://www.imperva.com/learn/application-security/social-engineering-attack/

43. 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 MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
2. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.