ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
підпис
«__30__» ____08____ 2024 р.

СИЛАБУС

Навчальна дисципліна: "Функційна безпека інформаційно комп'ютерних систем"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: другий (магістреський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Стецюк Микола Васильович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/sklad-kafedry/
E-mail викладача(ів)	mykola.stetsiuk@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=9012
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: http://surl.li/oidwzv * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр ІІ (зимово-весняний)
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	2	8	240	90	36	36	18	-	150	-	-	+	-

Анотація дисципліни

Дисципліна формує у студентів знання про сучасні операційні системи, забезпечення ідентифікації, аутентифікації та авторизації суб'єктів доступу в операційних системах, безпеці інформації в сучасних операційних системах, методи та засоби захисту інформації в сучасних операційних системах.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, застосування інформаційно-комп'ютерних технологій (інструменти та утиліти ОС Windows та Linux Ubuntu).

Пререквізити: технології програмування та алгоритмізації, основи інформаційної безпеки.

Кореквізити: безпека вебресурсів, захист інформації в інформаційно-комунікаційних системах

Мета і завдання дисципліни

Метою дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення функціональної безпеки та надійності інформаційно-комп'ютерних систем. Включає аудит, моніторинг та менеджмент безпеки систем; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань управління інцидентами та ризиками функціональної безпеки в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційно-комп'ютерних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери функціональної безпеки; інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) для забезпечення функціональної безпеки; системи управління функціональною безпекою; технології, методи, моделі та засоби забезпечення функціональної безпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Завдання дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки магістрів зі спеціальності «Кібербезпека та захист інформації»:

компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

результати навчання:

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти 4 уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
Студент, який успішно завершив вивчення дисципліни, повинен: застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки; аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту; аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою організації; забезпечувати безперервність бізнес/операційних процесів, а також аналізувати та оцінювати ризики для інформаційної безпеки організації; досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам; аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій; приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень; планувати навчання, використовувати методи комп‘ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки;

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	1. **Питання та визначення функційної безпеки** Визначення функційної безпеки. Мета функційної безпеки. Принципи функційної безпеки.	**ЛР №1** Дослідження операційних систем Windows та Linux. Налаштування, командний рядок, системні функції роботи з процесами та віртуальною пам’яттю	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	4	Літ.: [[1] с.12-25 [2] с.10-30 [3] с.20-40
2	**Архітектури операційних систем** Основні поняття концепції операційної системи. Архітектурні особливості будови сучасних операційних систем. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз.	-	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1.	4	[5] с.15-35 [7] с.21-26,47-54 [9] с.13-17,221-239 [10] с.24-28

3	**Ядро операційної системи** Складові частини ядра. Підходи до проектування ядра. Багаторівневі системи. Змішані системи.	**ЛР №2** Дослідження технології захисту цілісності даних RAID	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	4	[1] с.86-105 [7] с.12-26 [10] с. 17-29
4	**Файлові системи операційних систем** Файлова система NTFS. Архітектура файлової системи EFS. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS. RAID-масиви	-	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	4	[1] с.474-506 [5] с.105-121 [7] с.29-33 [9] с.186-219 [10] с.35-59
5	**Сутність проблеми захисту операційних систем** Вимоги, що висуваються до захищених операційних систем. Поняття та призначення політики інформаційної безпеки. Порушення політики інформаційної безпеки. Атаки на рівні операційної системи.	**ЛР №3** Дослідження та розробка алгоритмів антивірусного програмного забезпечення. Протидія вірусам в операційній системі Windows	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	5	[2] с.11-39 [3] с.5-60 [6] с.23-60 [22] с.593-602
6	**Найпоширеніші загрози безпеці операційних систем** Несанкціонований доступ. Незаконне використання привілеїв. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи". Шкідливе програмне забезпечення.	-	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	5	[2] с.373-378 [3] с.5-60,240-256
7	**Технології боротьби з вірусами в операційних системах** Ознаки інфікованої операційної системи. Технології виявлення вірусів. Класифікація антивірусного програмного забезпечення.	**ЛР №4** Шифрування файлів в файловій системі NTFS	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	4	[2] с.463-499 [3] с.240-256 [6] с.71-87 [17]

8	**Сучасні технології ідентифікації користувачів операційних систем** Парольна технологія ідентифікації. Апаратна технологія ідентифікації. Біометрична технологія ідентифікації. Багатофакторна ідентифікація.	-	Опрацювання теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	4	[2] с.272-278 [3] с.94-114 [6] с.53-60
9	**Організація безпеки операційної системи Windows** Компоненти системи захисту ОС Windows. Механізм захисту об'єктів ОС Windows. Ідентифікатор захисту. Маркери доступу. Дескриптори захисту. Права та привілеї (суперпривілеї) облікових записів. Типові права користувачів ОС Windows.	**ЛР №5** Розмежування прав доступу в операційній системі Windows, політики безпеки Windows	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	4	[8] [9] [11] [22] с.966-975
10	**Аудит безпеки операційної системи Windows** Категорії аудиту безпеки. Процес входу користувача в операційну систему. Політика обмеженого використання програм. Резервування в ОС Windows	-	Опрацювання теоретичного матеріалу лекції №10. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	4	[3] с.256-268 [21] с.383-407
11	**Конфігурація та моніторинг операційної системи Windows** Запуск від імені адміністратора, локальні користувачі та домени. CLI і PowerShell. Інструмент керування Windows, диспетчер завдань і монітор ресурсів. Доступ до мережевих ресурсів. Windows Server.	**ЛР №6** Налаштування аудиту безпеки в операційній системі Windows, засоби резервування	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4	[8] [14] [19]
12	**Політики безпеки операційної системи Windows (частина 1)** Політики облікових записів. Локальні політики. Монітор брандмауера для програми Windows Defender. Політика диспетчера списку мереж.	-	Опрацювання теоретичного матеріалу лекції №12. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4	[8] [11] [26]

13	**Політики безпеки операційної системи Windows: (частина 2)** Політика відкритого ключа. Політика управління додатками. Політика IP-безпеки на «Локальний комп'ютер». Конфігурація розширеної політики аудиту.	**ЛР №7** Керування політиками в операційній системі Windows	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	4	[8] [11] [15] [22]
14	**Організація безпеки операційної системи Linux** Модель безпеки операційної системи Linux. Підсистема ідентифікації та аутентифікації. Підсистема розмежування доступу. Монітор безпеки.	-	Опрацювання теоретичного матеріалу лекції №14. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	4	[4] с.75-84 [6] [8] [10] с.31-33,90-102 [22] с. 798-802
15	**Технології підвищення рівня захищеності операційної системи Linux** Linux з покращеним рівнем безпеки (SELinux). Система мандатного контролю доступу AppArmor. Система забезпечення мандатного контролю доступу TOMOYO Linux. Резервування в ОС Linux.	**ЛР №8** Розмежування прав доступу в операційній системі Linux	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	4	[1] с.31-34 [4] с.75-84 [13] с. 96-118 [20]
16	**Робота на хості Linux** Процеси та форки. Зловмисне програмне забезпечення на хості Linux. Перевірка руткіта.	-	Опрацювання теоретичного матеріалу лекції №16. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	4	[1] с.167-197 [8]
17	**Організація безпеки операційної системи Android** Модель безпеки ОС Android. Ідентифікації та аутентифікації. Розмежування доступу. Стандартні та спеціальні дозволи.	**Тестування**	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	6	[1] с.50-52 [5] с.30-36 [22] с.838-844

18	**Організація безпеки операційної системи iOS** Архітектура операційної системи iOS. Модель безпеки операційної системи iOS. Характеристика функціонування компонентів Secure Enclave та TouchID.		Опрацювання теоретичного матеріалу лекції №18. Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	6	[1] с.50-56 [7] с. 54-58

*** лекції проводяться по 2 години щотижня;**
**** лабораторні проводяться по 4 години раз в 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, 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://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. 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	Тестування	Залік за рейтингом
Тема	1-4	1-5	
Ваговий коефіцієнт	0,8	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 звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні 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 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	1–10	11–14	15–17	18–20
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 20 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 20 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 не пізніше ніж через 10 днів після проходження тестування.

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

Семестровий контроль (залік).

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.
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	***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	***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. Призначення та функції.
2. Класифікація сучасних операційних систем.
3. Тенденції в розвитку ОС.
4. Технології проектування.
5. Основні поняття концепції операційної системи.
6. Архітектурні особливості будови сучасних операційних систем.
7. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз.
8. Складові частини ядра.
9. Підходи до проектування ядра.
10. Багаторівневі системи.
11. Змішані системи.
12. Файлова система NTFS.
13. Архітектура файлової системи EFS.
14. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS.
15. RAID-масиви
16. Вимоги, що висуваються до захищених операційних систем.
17. Поняття та призначення політики інформаційної безпеки.
18. Порушення політики інформаційної безпеки.
19. Атаки на рівні операційної системи.
20. Несанкціонований доступ.
21. Незаконне використання привілеїв.
22. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи".
23. Шкідливе програмне забезпечення.
24. Ознаки інфікованої операційної системи.
25. Технології виявлення вірусів.
26. Класифікація антивірусного програмного забезпечення.
27. Парольна технологія ідентифікації.
28. Апаратна технологія ідентифікації.
29. Біометрична технологія ідентифікації.
30. Багатофакторна ідентифікація.
31. Компоненти системи захисту ОС Windows.
32. Механізм захисту об’єктів ОС Windows.
33. Ідентифікатор захисту.
34. Маркери доступу.
35. Дескриптори захисту.
36. Права та привілеї (суперпривілеї) облікових записів.
37. Типові права користувачів ОС Windows.
38. Категорії аудиту безпеки.
39. Процес входу користувача в операційну систему.
40. Політика обмеженого використання програм.
41. Резервування в ОС Windows
42. Запуск від імені адміністратора, локальні користувачі та домени.
43. CLI і PowerShell.
44. Інструмент керування Windows, диспетчер завдань і монітор ресурсів.
45. Доступ до мережевих ресурсів.
46. Windows Server.
47. Політики облікових записів.
48. Локальні політики.
49. Монітор брандмауера для програми Windows Defender.
50. Політика диспетчера списку мереж.

51. Політика відкритого ключа.
52. Політика управління додатками.
53. Політика IP-безпеки на «Локальний комп'ютер».
54. Конфігурація розширеної політики аудиту.
55. Модель безпеки операційної системи Linux.
56. Підсистема ідентифікації та аутентифікації.
57. Підсистема розмежування доступу.
58. Монітор безпеки.
59. Linux з покращеним рівнем безпеки (SELinux).
60. Система мандатного контролю доступу AppArmor.
61. Система забезпечення мандатного контролю доступу TOMOYO Linux.
62. Резервування в ОС Linux.
63. Процеси та форки.
64. Зловмисне програмне забезпечення на хості Linux.
65. Перевірка руткіта.
66. Модель безпеки ОС Android.
67. Ідентифікації та аутентифікації.
68. Розмежування доступу.
69. Стандартні та спеціальні дозволи.
70. Архітектура операційної системи iOS.
71. Модель безпеки операційної системи iOS.
72. Характеристика функціонування компонентів Secure Enclave та TouchID.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни “Операційні системи та технології їх захисту” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі Moodle

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Safety and Security of Cyber-Physical Systems by Frank J. Furrer, Oliver Goerlitz, Norbert Pohlmann. Springer, 2021. 450 p.
2. Security and Resilience in Cyber-Physical Systems by Masoud Tabib, Mahdi Zareapoor. Elsevier, 2022. 300 p.
3. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. Київ: КНУ, 2021. 412 с.
4. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by Eric D. Knapp, Joel Thomas Langill. Elsevier, 2021. 400 p.
5. Safety-I and Safety-II: The Past and Future of Safety Management by Erik Hollnagel. CRC Press, 2021. 240 p.
6. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Одеса: ОНУ, 2020. 350 с.
7. Захист інформації в комп'ютерних системах / І.А. Терейковський, С.О. Гнатюк. Харків: ХНУРЕ, 2020. 300 с.
8. Practical Industrial Cybersecurity: ICS, SCADA, and IIoT by Pascal Ackerman. Packt Publishing, 2021. 450 p.
9. Cyber-Physical Systems: Foundations, Principles and Applications by Houbing Song, Danda B. Rawat, Sabina Jeschke, Christian Brecher. Academic Press, 2022. 500 p.
10. Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense by Javier Lopez, Roberto Setola, Stephen D. Wolthusen. Springer, 2021. 420 p.
11. Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework by Jonathan Reuvid. Routledge, 2022. 300 p.
12. Risk Management Framework: A Lab-Based Approach to Securing Information Systems by James Broad, James W. Graves. Syngress, 2021. 350 p.

Додаткова

1. Оцінка ризиків в інформаційних системах / О.В. Гайдай, Ю.М. Гончарова. Дніпро: ДНУ, 2021. 275 с.
2. Cybersecurity Audit: Developing a Successful Program by Douglas J. Landoll. Auerbach Publications, 2022. 450 p.
3. Audit and Assurance Services by Alvin A. Arens, Randal J. Elder, Mark S. Beasley. Pearson, 2021. 720 p.
4. Аудит інформаційної безпеки / П.І. Колесник, М.М. Гуменюк. Львів: Видавництво Львівської політехніки, 2022. 230 с.
5. Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson. Wiley, 2021. 1200 p.
6. Computer Security: Principles and Practice by William Stallings, Lawrie Brown. Pearson, 2022. 800 p.
7. Trends in Cybersecurity: Critical Infrastructure and the Next Generation of Threats by Larry Clinton. Routledge, 2022. 280 p.
8. Cybersecurity Threats, Malware Trends, and Strategies by Nicholas Antill. Syngress, 2021. 320 p.
9. Сучасні проблеми та тенденції розвитку інформаційної безпеки / В.П. Петров, І.О.

Соловйов. Київ: КНУ, 2022. 240 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php.