ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

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

СИЛАБУС

Навчальна дисципліна: "*Системи контролю доступу*"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: Перший бакалаврський

Загальна інформація

Позиція	Інформація
Викладач(і)	Муляр Ігор Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/mulyar-igor-volodymyrovych
E-mail викладача(ів)	muliariv@khmnu.edu.ua
Контактний телефон	+3 8 067 938-15-44
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=6751
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр II (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	3	6	6	180	85	34	51			95				+

Анотація дисципліни

Дисципліна «Системи контролю доступу» – одна з фундаментальних дисциплін професійної підготовки бакалаврів зі спеціальності „Кібербезпека". Дисципліна викладається для студентів очної денної форми навчання. При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, проектні, продуктивні, проблемні, контекстні, застосування інформаційно-комп'ютерних технологій (САПР IP Video System Design Tool, AutoCad, Cisco packet tracer, тощо).

Пререквізити: технічний і криптографічний захист інформації.

Кореквізити: проєктно-технологічна практика; комплексні системи захисту інформації.

Анотація дисципліни

Дисципліна «Системи керування доступом» - одна з фундаментальних дисциплін професійної підготовки бакалаврів зі спеціальності „Кібербезпека”.

При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, проектні, продуктивні, проблемні, контекстні, застосування інформаційно-комп’ютерних технологій (САПР IP Video System Design Tool, AutoCad, Cisco packet tracer, тощо).

Пререквізити: технічний і криптографічний захист інформації

Кореквізити: Комплексні системи захисту інформації

Мета і завдання дисципліни

Мета дисципліни. Формування системи знань та розуміння предметної області необхідних для формалізованого опису, аналізу й синтезу комплексних систем захисту інформації; розв’язування складних спеціалізованих задач; застосування методів та засобів проектування, випробування, сертифікації систем контролю доступу.

Предмет дисципліни. Методи, методики, інформаційно-комунікаційні технології, програмно-апаратне забезпечення систем контролю доступу, їх сертифікації та супроводу.

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

компетентності:

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

результати навчання:

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

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

Студент, який успішно завершив вивчення дисципліни, повинен: *аналізувати, виявляти та оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам та *проводити оцінку* ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах, *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *вирішувати* задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів в інформаційно-телекомунікаційних (автоматизованих) системах, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *вирішувати* задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, *виконувати* моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, *використовувати* отримані результати для ефективного рішення спеціалізованих задач дисципліни і професійної діяльності; *забезпечувати* введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема лабораторної роботи**	Самостійна робота студента		
				Зміст	Години	Літера-тура
1	*2*	*3*	*4*	*5*	*6*	*7*
1	1	***Загальні положення про дисципліну*** Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Визначення, позначення та скорочення. Поняття та призначення СКД	**ЛР1.** Аналіз структури об'єкту захисту та оцінка можливих загроз, уразливостей та дестабілізуючих чинників. .	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1.	5	Літ.:[1] с.6-8; [2] с.81-86; [3] с.500-515; [10] с.1-48; [11] с.2-13; [17]
2	1	**Призначення та характеристики СКД** Визначення, позначення та скорочення. Поняття та призначення СКД. Основні вимоги до СКД. Головні принципи та етапи захисту. Завдання		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1.	6	[Літ.:[3] с.26-36; [4] с.140-191; [10] с.19-49

		та функції СКД. Адміністрація Державної служби спеціального зв'язку та захисту інформації України.				
3	1	**Програмні засоби системи контролю доступу.** Використання програмних комплексів захисту інформаційних ресурсів Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Класифікація. ПЗ. Організація захисту у ОС. Керування правами Windows Active Directory. SELinux.	**ЛР2.** Оперативний центр безпеки (SOC). Дослідження можливих загроз та операцій по захисту від них	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2.	5	[Літ.:[1] с.6-16; [2] с.189-199; [10] с.19-49; [11] с.13-25; [16]; [17]; [18]
4	1	**Оперативний центр безпеки** Архітектура та загальні особливості операційних центрів безпеки (SOC). Завдання захисту програм та інформації. Класифікацію загроз, типи. Матриця атак MITRE ATT&CK. Defense & Intelligence | MITRE. Команда реагування на комп'ютерні надзвичайні події. CERT-UA		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2.	6	Літ.:[1] с.6-16; [2] с.189-199; [10] с.19-49; [11] с.13-25; [16]
5	1	**Управління інформаційною безпекою**	**ЛР3**. Використанння SIEM Splunk для відслідковування,	Опрацювання теоретичного матеріалу,	5	Літ.:[3] с.23-54; [5] с.101-130;

		Система управління інформаційною безпекою (SIM). Система управління подіями безпеки (SEM). Система збору та кореляції подій безпеки (SIEM). Фукціональність систем. Приклади використання. Журналювання даних і генерації звітів. Splunk SIEM. Система запобігання витоку конфіденційної інформації (DLP). Структура. Принципи побудови. Механізми визначення ступеня конфіденційності документа.	логування загроз і візуалізації	підготовка до виконання ЛР3.		[9] с.18-49
6	1	**Компоненти СКД (частина 1)** Контролери. Автономні контролери. Мережеві контролери. Ідентифікатори. RFID.		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3.	6	Літ.:[2] с.148-186; [3] с.31-38; [6] с.90-116
7	1	**Компоненти СКД (частина 2)** Зчитувачі. Стандарт EM-Marine. Стандарт Mifare. Зчитувачі дальньої дії (UHF). Біометричні зчитувачі. Виконавчі пристрої. Електрозамки. Кнопки виходу. Турнікети. Дверні доводчики	**ЛР4**. Утворення системи контролю і захисту приміщень на основі IoT пристроїв Xiaomi (модулів розумного будинку) та давачів охоронної сигналізації.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4.	5	Літ.:[2] с.187-200; [3] с.38-68; [6] с.116-130
8	2	**Основні принципи організації СКД** Принципи		Опрацювання теоретичного матеріалу,	6	[1] с.34-46; [2] с. 46-63;

		організації СКД. Концептуальні підходи до проєктування систем захисту. Порядок проведення робіт із створення СКД в інформаційно-телекомунікаційній системі (ІТС). Етапи створення КСЗІ в ІТС.		підготовка до захисту ЛР №4.		[3] с.328-343
9	2	**Етапи створення СКД** Формування технічного завдання на створення СКД в ІТС. Базові розділи ТЗ. Нормативний супровід розробки ТЗ. Вимоги НД ТЗІ 3.7-001-99 до змісту, послідовності та викладення розділів ТЗ. Розробка ескізного проєкту СКД. Представлення схем, структур, елементів СКД. Оформлення та представлення текстової документації. Розробка комплекту документації для етапу проєктування СКД. КСЗІ в критичній інфраструктурі.	**ЛР5.** Організація та використання систем відеомоніторингу контрольованої території.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5.	5	Літ.:[1] с.17-26; [2] с. 18-34; [3] с.316-327
10	2	**Зони забезпечення безпеки.** Поняття контрольованої зони. Класифікація та розташування зон забезпечення безпеки. Рубежі охорони. Пункти контролю доступу. Охоронні зони.		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5.	6	Літ.:[5] с.125-145; [7] с. 115-168 [12] с. 28-56

		Зони санітарної охорони та санітарно-захисні зони.				
11	2	**Системи відеоспостереження.** Методи та засоби відеоспостереження. Відеокамери та їх класифікація. Конструкція і основні характеристики цифрових та аналогових камер відеоспостереження. відеореєстратори, Принципи протидії засобам відеорозвідки.	**ЛР6.** Розробка системи відеоспостереження на основі устаткування фірми Hikvision	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6.	5	Літ.:[1] с.126-144; [2] с. 116-163 [7] с.228-243]
12	2	**Пристрої, фізична та апаратна безпека IoT** Вступ. Терміни та визначення безпеки Інтернету речей. Архітектура та еталонні моделі IoT. Стандарти, протоколи, стейкхолдери в IoT Пристрої та їх характеристики. Безпека зберігання даних. Розумний будинок. Застосування технологій розумного будинку при побудові СКД.		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6.	6	Літ.: [5] с.62-108; [9] с.4-110; [24]; [28]

13	2	**Системи пожежної сигналізації.** Загальні відомості про системи пожежної сигналізації. Теплові і пожежні сповіщувачі. Пожежні сповіщення полум'я. Димові оптично-електронні пожежні сповіщувачі. Димові радіоізотопні пожежні сповіщувачі. Приймальні станції пожежної сигналізації	**ЛР7** Проєктування системи контролю та управління доступом з використанням комплекту обладнання ZKTeco	Опрацювання теоретичного матеріалу, підготовка до до виконання ЛР7.	5	Літ.:[5] с.34-46; [7] с.83-90; [8] с.228-24724]
14	2	**Системи охоронної сигналізації.** Загальні відомості про системи охоронної сигналізації. Поняття і класифікація технічних засобів охоронної сигналізації. Застосування технічних засобів. Автономні та централізовані системи. Периметральні технічні засоби. Допоміжні технічні засоби.		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7.	6	Літ [2] с.199-250; [3] с.527-548; [10] с.67-101
15	2	**Системи блокування відеоспостереження** Принципи протидії засобам відеорозвідки. Класифікація візуально-оптичних	**ЛР8.** Сертифікація та забезпечення функціонування СКД, моніторинг роботи та технічний супровід.	Опрацювання теоретичного матеріалу, підготовка до до виконання ЛР8.	6	Літ.:[1] 126-128; [2] с.63-67; [3] с.506-527; [15]

		каналів витоку інформації. Методи захисту інформації від витоку по візуально-оптичному каналу. Методи і засоби пошуку прихованих відеокамер. Пошук і блокування прихованих пристроїв відеоспостереження				
16	2	**Методи та засоби забезпечення систем фізичного доступу та охорони території** Системи фізичного захисту об'єктів. Типова система фізичного доступу. Доглядові системи.. Ручні та арочні металошукачі. Автономні та мережеві системи доступу.		Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8. Підготовка до контрольної роботи.	6	Літ [2] с.199-250; [3] с.527-548; [10] с.67-101]
17	3	**Організація випробувань СКД** Реалізація СКД відповідно до вимог нормативно-правових документів. Аналіз та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. Забезпечення супроводу СКД в ІКС. Кадрові заходи. Державний контроль за станом	Підсумкове заняття.	Опрацювання теоретичного матеріалу.	6	Літ.: [2] с.189-198; [3] с.548-562; [11] с.111-134; [18]

		ТЗІ				
		Міжнародні стандарти та вимоги до СКД Європейська організації з кібербезпеки (ECSO). Агентство Європейського Союзу з кібербезпеки (ENISA). Директива NIS (Network and Information Security). Вимоги GDPR (General Data Protection Regulation). Прогалини у стандартах безпеки. Закон ЄС про кібербезпеку (EU cybersecurity Act). Схеми сертифікації.	Контрольна робота.			7] с.548-562; [14]; [16]; [17]

* лекції проводяться по 2 години.

** лабораторні роботи проводяться раз у два тижні 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, індивідуальну роботу та інші домашні завдання виконувати відповідно до графіка. Пропущену лабораторну роботу 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 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 у семестрі за ваговими коефіцієнтами

	Аудиторна робота	Контрольні заходи	Підсумковий контрольний захід
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-4	1-4	1-4
Ваговий коефіцієнт	0,4	0,2	0,4

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 контрольних робіт. Контрольна робота складається з теоретичного питання та практичного завдання за темою одного з практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно виконав поставлене практичне завдання.

Оцінку «добре» отримує студент, який допустив дві-три несуттєві помилки при відповіді на теоретичне питання та правильно виконав поставлене практичне завдання.

Оцінку «задовільно» отримує студент, який дав лише часткову відповідь на теоретичне питання або допустив суттєві помилки при виконанні практичного завдання.

Оцінку «незадовільно» отримує студент, який не зміг виконати практичне завдання або не дав відповіді на теоретичне питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

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

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.

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	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. Організаційні основи розробки проектів, реалізації та модернізації захищених інформаційних і комунікаційних систем.
2. Соціальні та морально етичні норми колективного розроблення проектів.
3. Правові норми організації роботи колективу для розробки проектів.
4. Оптимізація співробітництва у колективі при розробці проектів.
5. Загальна технологія розробки комплексів засобів захисту інформаційно-комунікаційних систем.
6. Призначення СКД.
7. Формування технічного завдання на створення СКД в ІТС.
8. Спеціалізоване програмне забезпечення.
9. Класифікація джерела загроз та загроз~~и~~ інформації.
10. Системи спостереження за транспортними засобами.
11. Програмно-апаратні та спеціальні комплекси.
12. Оперативний центр безпеки (SOC).
13. SIEM Splunk.
14. Матриця атак MITRE ATT&CK.
15. Засоби пошуку пристроїв перехоплення інформації, що використовують фізичні властивості навколишнього середовища.
16. Засоби відеоспостереження.
17. Архітектура та еталонні моделі IoT.
18. Системи пожежної сигналізації.
19. Системи охоронної сигналізації.
20. Системи фізичного захисту об’єктів.
21. Доглядові системи.
22. Контролери.
23. Ідентифікатори.
24. Зчитувачі.
25. Електрозамки.
26. Турнікети.
27. Біометричні зчитувачі.
28. Види спеціальних перевірок виділених приміщень.
29. Державне ліцензування діяльності в області захисту інформації.
30. Сертифікація засобів захисту інформації. Основні поняття.
31. Атестування об’єктів інформатизації. Основні поняття.
32. проекту
33. Етапи розробки СКД.
34. Принципи адаптації можливостей комплексу засобів захисту до вимог стандартів.
35. Вимоги нормативних документів щодо створення СКД в ІТС
36. Середовища функціонування ІТС. Вміст передпроєктних робіт щодо створення СКД.
37. Практика введення в дію СКД.
38. Схеми сертифікації.
39. Супровід СКД
40. Методи оцінки захищеності інформаційно-комунікаційних систем

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі на сторінці дисципліни https://msn.khmnu.edu.ua/course/

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Методологія захисту інформації. Аспекти кібербезпеки: навчальний посібник / Г.М. Гулак та інші. К.: Видавництво НА СБ України, 2020. 256 с.	http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf
2.	Системи пожежної та охоронної сигналізації : навч. посіб. / Кушнір А.П., Чалий Д.О. Львів : СПОЛОМ, 2022. 298 с.	https://sci.ldubgd.edu.ua/bitstream/123456789/10291/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf
3.	Проєктування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.	https://vlp.com.ua/node/20177
4.	Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. - 252 с	http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf
5.	Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; 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/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing
6.	Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.	https://msn.khnu.km.ua/course/view.php?id=5962
7.	Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.	https://www.pdfdrive.com/cyber-security-for-cyber-physical-systems-d187690371.html
8.	Терлецький Т. В., Федорчук-Мороз В. І., Кайдик О. Л. Системи пожежної сигналізації : Навчальний підручник для студентів технічних спеціальностей / під заг. ред. Т. В. Терлецького – Луцьк: ІВВ ЛНТУ, 2022. – 130 с.	http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
9.	Fundamentals of InformationSystems Security / Editors : David	https://www.pdfdrive.com/

	Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.	fundamentals-of-information-systems-security-d186521700.html
10.	Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software Level / Editors : Michael Schwartz, Maciej Machulak. – Apress, 2018. – 377 p.	https://www.pdfdrive.com/securing-the-perimeter-deploying-identity-and-access-management-with-free-open-source-software-e176342517.html
11.	Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu**. –** Taylor & Francis Group, 2016**. –** 564 p.	https://www.pdfdrive.com/security-and-privacy-in-internet-of-things-iots-models-algorithms-and-implementations-d175284726.html
12.	Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. – Cham, Switzerland : Springer, 2016. – 360 p.	https://www.pdfdrive.com/cyber-physical-security-e31483670.html

Додаткова

13.	Practical Information Security Management: A Complete Guide to Planning and Implementation/ Tony Campbell. – Australia: Burns Beach, 2016. – 253 p.	https://www.pdfdrive.com/practical-information-security-management-a-complete-guide-to-planning-and-implementation-d158204677.html
14.	Трегуб В.Г. Проектування систем автоматизації: Навч. посібник. − К.: Видавництво Ліра-К, 2017. − 344 с.	https://lira-k.com.ua/preview/12125.pdf
15.	Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual – Quantico, Virginia : Defense Counterintelligence and Security Agency, 2020. – 163 p.	https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA_Assessment_and_%20Authorization_Process_Manual_Version_2.1.pdf
16.	Yevseiev S. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes / S. Yevseiev, H. Kots, S. Minukhin, O. Korol, A. Kholodkova // Восточно-Европейский журнал передовых технологий. – 2017. – № 5(9). – С. 19-35	http://nbuv.gov.ua/UJRN/Vejpte_2017_5%289%29__4
17.	НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. – Чинний від 20 грудня 2000 р. – Київ : ДСТСЗІ СБ, 2000. – [8] с.	https://tzi.com.ua/downloads/3.6-001-2000.pdf
18.	НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. – Чинний від 12 грудня 2007 р. – Київ : ДСТСЗІ СБ, 2007. – [7] с.	https://tzi.com.ua/downloads/1.1-005-07.pdf
19.	НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від	https://tzi.com.ua/downloads/2.6-001-11.pdf

	несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Чинний від 25 березня 2011 р. – Київ : Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2011. – [130] с.	
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.	https://metrology.com.ua/ntd/skachat-dstu-gost-gost-r/dstu/dstu-iso-iec-27032-2016/
21.	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
22.	Муляр І.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С.В. Ленков, В.М. Джулій, І.В. Муляр // Сучасна спеціальна техніка. Науково практичний журнал. – ДНДІ МВС України, 2016 – Вип. №2(45). – С.59-66	http://elar.naiau.kiev.ua/handle/123456789/13673
23.	Муляр І.В. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В.М. Джулій, Б.М. Кізюн, І.В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. №63. – С. 51-60	http://elar.khnu.km.ua/jspui/handle/123456789/8085
24.	Stephen Sakawa Kibwage. Role-Based Access Control Administration of Security Policies and Policy Conflict Resolution in Distributed Systems / Stephen Sakawa Kibwage. – A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems Graduate School of Computer and Information Sciences. – Nova Southeastern University, 2015. – 111 p.	https://www.pdfdrive.com/role-based-access-control-administration-of-security-policies-and-policy-conflict-resolution-in-e96324096.html
25.	The Internet of Things: Do-It-Yourself Projects with Arduino, Rasberry Pi, and BeagleBone Black / Edited by Donald Norris. – McGraw-Hill Education, 2015. – 582 p.	https://www.pdfdrive.com/the-internet-of-things-do-it-yourself-projects-with-arduino-raspberry-pi-and-beaglebone-black-d176037121.html
26.	Гапак О. М., Болога С.І. Захист інформації в комп'ютерних системах : підручник. Ужгород : ДВНЗ «Ужгородський національний університет», 2021. 184 с.	https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36506/1/%d0%9f%d0%86%d0%94%d0%a0%d0%a3%d0%a7%d0%9d%d0%98%d0%9a%20%d0%97%d0%86%d0%9a%d0%a1_2021.pdf
27.	Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125.	https://www.researchgate.net/publication/332779915_Safeguarding_the_Information_Systems_in_an_Organization_through_Different_Technologies_Policies_and_Actions/link/5cc9228992851c8d22105ad8/download

28.	Information Security Standard: Information Technology Resource Management. Virginia Information Technologies Agency (VITA), 2016. – 183 p.	https://www.pdfdrive.com/information-security-standard-e60350584.html
29.	The Development of an Intelligent Complex of Radiation-Technological Control of a Safety Barrier / S. Lienkov, O. Banzak, Y. Husak, I. Muliar, V. Cheshun, E. Lenkov // International Journal of Emerging Trends in Engineering Research. – Volume 8. No. 7, July 2020. – P. 3483–3486.	https://www.scopus.com/authid/detail.uri?authorId=57192704936
30.	Довбня С. Створення системи технічного захисту інформації з використанням матриць небезпечних факторів, що характеризують технічні канали витоку / Сергій Довбня, Андрій Нікірін, Іван Четверіков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2014. – Вип. 1(27). – С. 14-21.	https://ela.kpi.ua/handle/123456789/17949

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/
2. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/

Розробник _____ к.т.н., доцент І.В.Муляр
Підпис Вчений ступінь, звання Ініціали, прізвище викладача(ів)

Погоджено

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

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