

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»

Лектор курсу		Котенко Андрій Миколайович, кандидат технічних наук, доцент кафедри систем інформаційного та кібернетичного захисту		Контактна інформація лектора (e-mail), сторінка курсу в Moodle		e-mail: 12z@ukr.net ; сторінка курсу в Moodle –	
Галузь знань		12 Інформаційні технології		Рівень вищої освіти		Магістри	
Спеціальність		Кібербезпека		Семестр		9	
Освітня програма		Магістр Кібербезпеки		Тип дисципліни		Професійної та практичної підготовки	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	12	-	18	12	80
АНОТАЦІЯ КУРСУ							
Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню		Компонентна база засобів технічного захисту інформації					
Освітні компоненти для яких є базовою							
Мета курсу:	Засвоєння методів та засобів здійснення контрольно-перепускного режиму на об'єкті інформаційної діяльності, який засновується на застосуванні обмежень відносно суб'єктів які пересікають межі ОІД.						
Компетентності відповідно до освітньої програми							
Soft- skills / Загальні компетентності (ЗК)				Hard-skills / Спеціальні компетентності (СК)			
ЗК-3. Знання інформаційних технологій – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах. ЗК-4. Навички керування проектами – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами.				ФК-1. Інтегративна компетентність ФК-3. Організаційно-комунікативна компетентність ФК-4. Професійна компетентність ФК-5. Загальнонаукова компетентність ФК-6. Політехнічна компетентність ФК-7. Інженерна компетентність			
Програмні результати навчання (ПРН)							
ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. ПРН 9. Уміти здійснювати вибір							

методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності.

ПРН-13. Уміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.

ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.

ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.

ПРН-24. Уміти здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності.

ПРН-25. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

ПРН-31. Уміти проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Змістовий модуль 1. «Загальна характеристика систем управління доступом»			
Тема 1. <i>Склад СКУД</i> Знати: Склад системи контролю та управління доступом на об'єкти інформаційної діяльності. Призначення системи контролю та управління доступом на об'єкти інформаційної діяльності у кібербезпеці. Вміти: Обґрунтовувати вибір засобів для обладнання еонтрольно-перепускного пункту на об'єкти інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. Формування компетенцій: ЗК1, ФК-1, ФК-5. Результати навчання: ПРН-25.	Лекція 1 2 год.	10	Лекція-візуалізація
	Практичне заняття 1 2 год.		Загальні положення. Обладнання перепускних пунктів
	Лабораторна 1. 2 год.		Дослідження методів обладнання перепускних пунктів

<p><u>Рекомендовані джерела:</u> 3-5,8.</p>	<p>Самостійна робота</p>		<p>УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року № 685/2021.</p>
<p>Тема 2. <i>Типи ідентифікаторів</i> <u>Знати:</u> Класифікацію СКУД. Методи ідентифікації людини. <u>Вміти:</u> обґрунтовувати вибір СКУД для конкретного об'єкту інформаційної діяльності. Обрати потрібний метод ідентифікації людини. Реалізувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. Володіти вмінням формувати технології розроблення СКУД на об'єкти інформаційної діяльності, розробляти проекти СКУД. <u>Формування компетенцій:</u>ЗК1, ЗК3, ФК-1, ФК-4, ФК-5 <u>Результати навчання:</u>ПРН-13, ПРН-17, ПРН-24, <u>Рекомендовані джерела:</u> 1,3-7,8,11,17,20,24,25.</p>	<p>Лекція 2 2 год</p>	<p>10</p>	<p>Лекція-візуалізація</p>
	<p>Практичне заняття 2 2 год</p>		<p>Склад засобів ідентифікації та автентифікації</p>
	<p>Практичне заняття 3 2 год</p>		<p>Ідентифікація по геометрії кісті рук</p>
	<p>Практичне заняття 4 2 год</p>		<p>Механічні засоби ідентифікації</p>
	<p>Лабораторн а 2. 2 год.</p>		<p>Дослідження способів порушення перепускного режиму та протидії</p>

	Самостійна робота		Реалізація системи контролю та управління доступом на об'єкти інформаційної діяльності. Здійснення вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності,
<p>Тема 3. Структури СКУД. Біометричні засоби ідентифікації особи</p> <p>Знати: Аналіз та класифікацію сучасних біометричних методів та засобів ідентифікації особи. Загальні відомості про засоби ідентифікації особи.</p> <p>Вміти: обґрунтовувати та реалізовувати системи контролю та управління доступом на об'єкти інформаційної діяльності, здійснювати вибір методів і засобів ідентифікації особи, здійснювати оцінку контролю та управління доступом, володіти вмінням формувати технології розроблення системи контролю та управління доступом на об'єкти інформаційної діяльності.</p> <p>Формування компетенцій: ЗК1, ЗК4, ФК-1, ФК-4, ФК-5.</p> <p>Результати навчання: ПРН-17, ПРН-24, ПРН-25.</p> <p>Рекомендовані джерела: 1,3-7,8,11,17,20,</p>	Лекція 3 2 год	7	Лекція-візуалізація
	Практичне заняття 5 2 год		Використання ідентифікаторів по ритму роботи на клавіатурі
	Лабораторна 3. 2 год.		Дослідження методів ідентифікації особи
	Самостійна робота		Галузь використання. Нормативні посилання. Класифікація пристроїв ідентифікації особи. Реалізація засобів ідентифікації особи систем контролю та управління доступом на ОІД. Здійснення оцінки систем контролю та управління доступом на ОІД відповідно до вимог діючих стандартів та нормативних документів.
<p>Тема 4. Динамічні методи біометричної ідентифікації</p> <p>Знати: Загальні положення. Організацію проведення перевірок стану СКУД та ТЗІ. Існуючі динамічні методи біометричної ідентифікації. Кваліфікація порушень СКУД. Висновки перевірок стану СКУД та критерії їх складання.</p> <p>Вміти: обґрунтовувати та реалізовувати системи захисту СКУД</p>	Лекція 4 2 год	7	Лекція-візуалізація
	Практичне заняття 6 2 год		Системи та обладнання СКУД. Обґрунтування та реалізація системи захисту СКУД на об'єктах інформаційної діяльності.

<p>на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. Використовувати положення про державний контроль за станом технічного захисту інформації. Затверджено Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87.</p> <p>Формування компетенцій:ЗК1, ЗК4,ФК-1, ФК-4, ФК-7.</p> <p>Результати навчання:ПРН-13, ПРН-18, ПРН-25.</p> <p>Рекомендовані джерела: 3-6,16,</p>	Лабораторна 4. 2 год.		Дослідження кодонабірних пристроїв
<p>Тема 5 <i>Контролери СКУД</i></p> <p>Знати: Типи контролерів СКУД. Існуючі структури СКУД.</p> <p>Вміти: Обирати потрібну структуру СКУД під конкретний тип об'єкту інформаційної діяльності. Обрати потрібний тип контролеру під визначену структуру СКУД. Провести оцінку функціонування розробленої СКУД.</p> <p>Формування компетенцій:ЗК1, ЗК3, ФК-1, ФК-5, ФК-8</p> <p>Результати навчання: ПРН-5, ПРН-24, ПРН-25, ПРН-31, ПРН-32</p> <p>Рекомендовані джерела: 1,7 ,11,17,20</p>	Лекція 5 2 год.	10	Лекція-візуалізація
Практичне заняття 7 2 год.	Принцип дії активних проксиміті-ідентифікаторів		
Практичне заняття 8 2 год.	Використання електричних замків та турнікетів на ОІД		
Лабораторна 5. 2 год.	Дослідження динамічних засобів ідентифікації		
Самостійна робота	Підсилена аутентифікація та ідентифікація. Адміністрування і система збору статистики. Існуючі структури СКУд. Мережевий контролер СКУД.		

<p>Тема 6. Виконавчі пристрої СКУД</p> <p>Знати: Існуючі виконавчі пристрої СКУД. Їх принцип функціонування. Стратегія технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>Вміти: Застосовувати знання при виборі виконавчих пристроїв СКУД.</p> <p>Формування компетенцій:ЗК1, ЗК4,ФК-1,ФК-6, ФК-7, ФК-8</p> <p>Результати навчання:ПРН-5, ПРН13, ПРН-17,ПРН-18, ПРН-22, ПРН-24, ПРН-32,</p> <p>Рекомендовані джерела: 2,4,6,9,14.</p>	Лекція 9 2 год	10	Лекція-візуалізація
	Практичне заняття 9 2 год		Виконавчі пристрої СКУД: електричні замки, електромеханічні замки, турнікети.
	Лабораторна а 9. 2 год.		Дослідження централізації контролерів СКУД
	Самостійна робота		Використання електричних замків. Принцип дії електромеханічного замка. Типи турнікетів.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Біометричний сканер, мережа Інтернет ауд. 423.
- Навчальна лабораторія засобів контролю доступу «HIK VISION»
- Програмне забезпечення.WindowsXP, 8,10, MicrosoftOffice.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Закони України:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-ХІІ
4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Укази президента:

5. № 685/2021 Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

6. Указ президента України №685/2021. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року
Постанова Кабінету Міністрів України
7. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
8. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.
Нормативні документи
9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
10. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. <https://zakon.rada.gov.ua/rada/show/v0215519-13>.
11. <http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327>

Основна

12. Bellifemine F, Caire G, Greenwood D (2007) Developing multi-agent systems with JADE. Wiley, London Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. № 1 (73). С. 86-89.
13. Benantar, Messaoud. (2006). Access control systems. Security, identity management and trust models. Access Control Systems: Security, Identity Management and Trust Models. 10.1007/0-387-27716-1.
14. Orange Pi. Wiring Op library. [Електронний ресурс]. – Режим доступу: <http://www.orange-pi.org/Docs/WiringPi.html>
15. Vysoven D. "Intelligent agent of access management and control system", International Competition of Student Scientific Works Black Sea Science 2020, Odessa, ONAFT 2020

***КРИТЕРІЙ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 бал
	• Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від екзамену
Додаткова оцінка	• Модульний контроль № 1 «Загальна характеристика систем управління доступом»	максимальна оцінка – 15 балів

РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 2 «Засоби СКУД»»	максимальна оцінка – 15 балів	
	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту	
	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	30 балів	
	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту	
Додаткова оцінка	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі.	30 балів	
ПІДСУМКОВЕ ОЦІНЮВАННЯ екзамен	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі.	30 балів	
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			Кри
бали	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Оцінка /затис в екзаменаційній відомості
90-100	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при	Достатній Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються	Відмінно / Зараховано (А)

	проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	порівняно з прикладами, що розглянуті при вивченні дисципліни	
82-89	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	Достатній Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (B)
75-81	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	Середній Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Добре / Зараховано (C)
64-74	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	Середній Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (D)
60-63	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Задовільно / Зараховано (E)
35-59	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	Незадовільний Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) <i>В залікову книжку не представляється</i>
- 3			