СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КЕРУВАННЯ ДОСТУПОМ В СИСТЕМАХ БЕЗПЕКИ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Факультет інформаційних технологій та кібербезпеки
Кафедра	Кафедра кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-19 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Корчинський Володимир Вікторович
vladkorchin @ukr.net

Професор кафедри кібербезпеки та технічного захисту інформації,
доктор технічних наук (спеціальність 05.13.21 – системи захисту інформації), професор

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Керування доступу в системах безпеки» має міждисциплінарний характер. Вона інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: фізика», програмування, іноземна фахова мова, комп'ютерні технології, теорія електричних кіл та електроніка, комп'ютерні мережі, теорія інформації та кодування. Теоретичні знання супроводжуються лабораторними та практичними роботами, на яких студенти опановують різні програмні та апаратні технології керування доступом, що стосується ідентифікації, аутентифікації, авторизації, підзвітності. У зв'язку цим розглядаються: методи доступу до файлів ОС; середовище розробки та програмування

	платформи ARDUINO для засобів ідентифікація і автентифікація суб'єктів та об'єктів; стандарти радіочастотної ідентифікації RFID; програмування приладу електронної ідентифікація iButton на основі системи Arduino; біометрична ідентифікація і автентифікація суб'єктів; засоби та інструменти організації єдиного входу і аутентифікації SSO; управління доступом на основі штрихового и QR кодування.
Мета дисципліни	– формування системних знань та розвиток умінь необхідних майбутнім фахівцям в галузі інформаційних технологій, щодо механізмів управління безпекою процесів взаємодії користувачів з системами і ресурсами та систем між собою.
Компетентності, формуванню яких сприяє дисципліна	Загальні: КЗ 1. Здатність застосовувати знання у практичних ситуаціях; КЗ 2. Знання та розуміння предметної області та розуміння професії; КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; Фахові: КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 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 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

	ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.ПРН22-24 ПРН 28. Аналізувати та проводити оцінку 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. ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

Обсяг дисципліни	Загальний обсяг дисципліни: 5 кредитів ЄКТС 150 годин). Для денної форми навчання: лекції – 20 годин, практичні заняття –14 години, лабораторні заняття –14 години, самостійна робота – 102 годин.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 6-му семестрі

Програма дисципліни

Тема 1.	***Цілі та задачі керування доступом, основні поняття*** Основні поняття та категорії «керування доступом», вимоги щодо якості забезпечення доступом. Ідентифікація та аутентифікація. Основні концепції управління доступом. Роль каталогів для завдань управлінні ідентифікацією.
Тема 2.	**Моделі керування доступом** Поняття моделі керування доступом. Дискреційне, мандатне та рольове управління доступом.
Тема 3.	**Технологія керування доступом** Керування доступом на основі правил. Обмежений користувацький інтерфейс. Матриця контролю доступу. Контентно-залежне керування доступом.
Тема 4.	**Адміністрування доступу** Централізоване адміністрування керування доступом. Мережний протокол RADIUS. Протокол TACACS.
Тема 5.	**Децентралізоване адміністрування керування доступом** Протокол Diameter. Децентралізоване адміністрування керування доступом
Тема 6	**Методи керування доступом** Рівні управління доступом. Адміністративний рівень. Політики і процедури управління доступом.
Тема 7	**Фізичний рівень керування доступом** Фізичні заходи безпеки: сегментація мережі; захист периметра; управління комп'ютерами; відділення робочих областей; резервне копіювання даних; прокладка кабелів; контрольовані зони. Технічний рівень: аудит шифрування і протоколи; доступ до мережі; мережева архітектура; доступ до систем.
Тема 8	**Типи керування доступом** Аналіз типів керування доступом. Превентивні: адміністративні. Превентивні: фізичні; технічні.
Тема 9	**Аналіз журналів реєстрації подій** Вимоги до журналу реєстрації подій. Інструменти аналізу журналу реєстрації подій. Моніторинг натискання клавіш. Захист даних аудиту і журналів реєстрації подій. Практика управління доступом.
Тема	**Моніторинг керування доступом** Виявлення вторгнень. IDS рівнів мережі та хоста. Виявлення вторгнень на основі знань або сигнатур. IDS на основі стану. Виявлення

10-11	вторгнень на основі статистичних аномалій. IDS на основі аномалій протоколів. IDS на основі аномалій трафіку. IDS на основі правил. Сенсори IDS. Мережевий трафік. Системи запобігання вторгнень. Хости-приманки. Мережеві сніфери.

Список рекомендованих джерел

1. Шон Харрис. CISSP Посібник для підготовки до іспиту / Шон Харрис // П’ята редакція, 2019. - 875 с.
2. Конспект лекцій з дисципліни Керування доступу в системах безпеки підприємств. Корчинський В.В. ДУІТЗ, 2022 р.
3. Практикум до лабораторних робіт з дисципліни Керування доступу в системах безпеки підприємств. Корчинський В.В. ДУІТЗ, 2022 р.
4. Практикум до практичних робіт з дисципліни Керування доступу в системах безпеки підприємств. Корчинський В.В. ДУІТЗ, 2022 р.
5. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина 1: лаб. практ. – Одеса: ОНАЗ ім. О.С. Попова, 2011.
6. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.

Інформаційні ресурси:

1. Біометрична система контролю та управління доступом. [Електронний ресурс]. – Режим доступу: https://vashtvmir.ru/biometricheskaya-sistema-kontrolya-i-upravleniya-dostupom-skud/.
2. Access control systems. [Електронний ресурс]. – Режим доступу: https://isbc.com/app_area/humans-id/access-control/.

Інформація про консультації

Щоп’ятниці у вересні-грудні 2023 року з 14^{20} до 15^{40} год., https://us02web.zoom.us/j/6197950058?pwd=YllCUkYwYlZYYU9rYmdsOUNTN3RlQT09 – проф. В.В. Корчинський

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		

0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням …….