СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека
Назва освітньо-наукової програми	«Кібербезпека»
Рівень вищої освіти	Третій (освітньо-науковий) рівень підготовки докторів філософії
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – доктор філософії Кваліфікація – доктор філософії з кібербезпеки
Кафедра	Кафедра кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-5 ОНП «Кібербезпека»
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 до інформаційних ресурсів» інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: кіберфізична безпека об'єктів критичної інфраструктури, комплексні системи безпеки, методологія забезпечення безперервності бізнес/операційних процесів сучасних підприємств, законодавство в області інформаційної безпеки, методи та засоби захисту інформації.

Предмет навчання дисципліни полягає у формуванні у аспірантів комплексних знань про сучасні тенденції розвитку інтелектуальних мереж, їх структуру, наявні механізми керування доступом до інформаційних ресурсів та

	заходи забезпечення безпеки інформації під час її зберігання та передавання. **Основними цілями вивчення дисципліни** є освоєння принципів побудови та функціонування інтелектуальних мереж, розподілу функцій керування послугами, а також ознайомлення з механізмами керування доступом до інформаційних ресурсів та забезпечення захисту інформації під час її зберігання та передавання по каналам зв'язку.
Мета дисципліни	– набуття знань щодо сучасних тенденцій та методів керування доступом до інформаційних ресурсів.
Компетентності, формуванню яких сприяє дисципліна	ЗК-5. Здатність розв'язувати комплексні проблеми у сфері кібербезпеки та інформаційної безпеки на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності. СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та інформаційної безпеки і дотичних міждисциплінарних напрямах та можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та інформаційної безпеки. СК-2. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в сфері кібербезпеки та інформаційної безпеки і дотичні міждисциплінарні проекти. СК-4. Здатність ефективно застосовувати методи аналізу, математичне моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових досліджень у сфері кібербезпеки та інформаційної безпеки. СК-6. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та інформаційної безпеки, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. СК-7. Здатність проектувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології, зокрема, комплексні системи криптографічного і технічного захисту інформації.
Результати навчання	РН-1 Мати передові концептуальні та методологічні знання з кібербезпеки та інформаційної безпеки і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки, IT-інфраструктур та інформаційних технологій, отримання нових знань та/або здійснення інновацій. РН-2 Планувати і виконувати теоретичні та/або експериментальні дослідження з кібербезпеки та інформаційної безпеки і дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН-3 Глибоко розуміти загальні принципи та методи кібербезпеки та інформаційної безпеки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці. РН-7 Застосовувати загальні принципи та методи математики, комп'ютерних та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для проведення наукових досліджень у

	сфері кібербезпеки та інформаційної безпеки. РН-8 Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у сфері кібербезпеки та інформаційної безпеки і дотичних міждисциплінарних напрямах. РН-10 Досліджувати, проектувати, впроваджувати і застосовувати сучасні інформаційні та безпекові технології, зокрема, методи та засоби криптографічного та технічного захисту інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: 6 кредитів ЄКТС (180 годин). Для денної та вечірньої форми підготовки: лекції – 30 годин, практичні заняття –30 годин, самостійна робота – 120 годин.
Форма підсумкового контролю	Іспит
Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі (18 тижнів)

Програма дисципліни

Лекції

Тема 1.	**Вступ до дисципліни «Керування доступом».** Визначення та основні поняття. Значення механізмів керування доступом у сучасному інформаційному суспільстві
Тема 2.	**Моделі доступу.** Дискреційний, мандатний, ролевий та інші моделі доступу. Порівняння різних моделей та їх застосування в реальних системах.
Тема 3.	**Методи аутентифікація.** Основні принципи та методи. Технічні засоби забезпечення аутентифікації: методи аутентифікація та авторизація.
Тема 4	**Методи авторизації.** Централізована та розподілена авторизація, принципи ACL та RBAC.
Тема 5.	**Управління правами доступу.** Створення, зміна та видалення прав доступу. Методи та практики управління правами користувачів.
Тема 6	**Аудит доступу.** Системи реєстрації подій та їх аналіз.
Тема 7	**Захист від несанкціонованого доступу.** Виявлення та запобігання атакам на систему доступу. Заходи безпеки для запобігання проникненню

Тема 8	**Впровадження системи керування доступом.** Ключові етапи та стратегії впровадження.
Тема 9	**Технічні засоби керування доступом.** Системи управління ідентифікацією та авторизацією.
Тема 10	**Практичні аспекти керування доступом.** Розгляд кейсів та прикладів реалізації систем керування доступом. Впровадження та підтримка систем у реальних середовищах
Тема 11	Регулювання та відповідність: Правові аспекти керування доступом, стандарти безпеки.
Тема 12	Підвищення безпеки через керування доступом: Застосування штучного інтелекту та аналізу даних для підвищення безпеки.
Тема 13	Тенденції у розвитку систем керування доступом: Централізовані та розподілені підходи, обліковий запис.
Тема 14	Ефективність та масштабованість систем доступу: Виклики та стратегії їх подолання.
Тема 15	Етичні аспекти у керуванні доступом: Захист приватності та дотримання етичних норм.
	Практичні заняття
Тема 1.	**Налаштування системи керування доступом.** Встановлення та конфігурація основних компонентів системи.
Тема 2.	**Створення користувачів та груп.** Створення облікових записів користувачів та надання їм відповідних прав доступу.
Тема 3.	**Налаштування політик безпеки.** Встановлення правил доступу та обмежень для різних категорій користувачів.
Тема 4	**Налаштування аудиту доступу.** Активація та налаштування механізмів реєстрації подій для аналізу доступу.
Тема 5.	**Впровадження механізмів двофакторної аутентифікації.** Налаштування та тестування систем аутентифікації на основі чогось, що ви знаєте та що маєте.
Тема 6	**Створення ролей та правил доступу.** Визначення ролей користувачів та надання їм відповідних прав доступу.
Тема 7	**Застосування групової політики.** Налаштування та впровадження політик, що об'єднують групи користувачів.
Тема 8	**Проведення аналізу аудиту доступу.** Аналіз журналів подій для виявлення потенційних порушень безпеки.

Тема 9	**Розробка та впровадження плану контролю доступу.** Визначення стратегій контролю доступу та впровадження їх у практичному середовищі.
Тема 10	**Тестування механізмів безпеки.** Виконання пенетраційного тестування для перевірки ефективності заходів безпеки.
Тема 11	**Імплементація механізмів одноразових паролів.** Налаштування та тестування системи, що використовує одноразові паролі для аутентифікації.
Тема 12	**Розгляд кейсів успішної інтеграції систем керування доступом.** Вивчення прикладів впровадження систем керування доступом у великих організаціях.
Тема 13	**Підготовка плану реагування на інциденти безпеки.** Розроблення та впровадження плану дій у випадку виявлення порушень безпеки.
Тема 14	**Оцінка впливу змін у правилах доступу.** Аналіз впливу змін у правилах доступу на роботу системи та її безпеку.
Тема 15	**Вивчення етичних аспектів у керуванні доступом.** Обговорення етичних проблем та вирішення конфліктів, пов'язаних з керуванням доступом

Список рекомендованих джерел

Рекомендована література:

1. Конспект лекцій з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р
2. Практикум до лабораторних робіт з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р.
3. Практикум до практичних робіт з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р.
4. 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.
5. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

Допоміжна

1. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23 лютого 2006 р. No 3475-IV-ВР//ВВР. – 2006. – № 30 (в редакції Закону № 1194-VII від 09.04.2014). – С. 258.

3. Юдін О. К. Правові аспекти формування системи державних інформаційних ресурсів [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Безпека інформації. – 2014. – Т. 20 (1). – С. 76–82.

2. Юдін О. К. Аналіз загроз державним інформаційним ресурсам [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 93–99.

3. Концепції формування системи національних електронних інформаційних ресурсів: розпорядження Кабінету Міністрів України від 5 травня 2003 р. № 259-р.

4. Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : затверджено Постановою Кабінету Міністрів України від 3 серпня 2005 р. No 688.
5. Юдін О. К. Загрози державним інформаційним ресурсам: терміни та визначення / О. К. Юдін, С. С. Бучик // Захист інформації. – 2014. – Т. 16 (2). – С. 121–125.

Інформаційні ресурси:

1. What is Information Resources . [Електроний ресурс]. – Режим доступу: https://www.igi-global.com/dictionary/information-resources/35622/.
2. Управління політикою доступу до мережних ресурсів . [Електроний ресурс]. – Режим доступу: http://referat-ok.com.ua/work/upravlinnja-politikoju-dostupu-do-mere/.

Інформація про консультації

Щопонеділок у лютому-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.**