СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

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	Другого (магістерського) рівня
Факультет	Факультет інформаційних технологій та кібербезпеки
Кафедра	Кафедра кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-4** 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: безпека телекомунікацій і комп'ютерних мереж, теорія інформації та кодування, законодавство в області інформаційної безпеки, методи та засоби захисту інформації, криптографічний захист інформації, безпека і експлуатація мережних і хмарних технологій» Предметом навчання дисципліни є формування у здобувачів системи знань щодо сучасного погляду на тенденції розвитку інтелектуальних мереж та структуру їх побудови, існуючі механізми управління доступом до інформаційних ресурсів та заходи забезпечення захисту інформації в процесі її зберігання та передавання.

	Основними завданнями вивчення дисципліни є набуття знань щодо принципів побудови та функціонування інтелектуальних мереж, поділу функцій керування послугами, механізмів управління доступом до інформаційних ресурсів та заходів забезпечення захисту інформації в процесі її зберігання та передавання по каналам зв'язку.
Мета дисципліни	– є набуття знань щодо принципів побудови, функціонування та захисту інтелектуальних мереж, механізмів доступу до інформаційних ресурсів на основі моделі інтелектуальної мережі і взаємодії основних її компонентів.
Компетентності, формуванню яких сприяє дисципліна	Загальні: КІ-1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ 1. Здатність застосовувати знання у практичних ситуаціях; КЗ 2. Здатність проводити дослідження на відповідному рівні.; КЗ 4. Здатність до абстрактного мислення, аналізу та синтезу. Фахові: 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. КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.
Результати навчання	РН 1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН 5. 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. РН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на

	об’єктах інформаційної діяльності та критичної інфраструктури. РН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН 12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН 23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредити ЄКТС (120 годин). Для денної форми навчання: лекції – 14 годин, практичні заняття –14 години, лабораторні заняття –12 години, самостійна робота – 80 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі (1–18 тижні)

Програма дисципліни

Тема 1.	Введення в дисципліну. Поняття інформаційних ресурсів та інтелектуальної мережі. Національні інформаційні ресурси. Правовий режим інформаційних ресурсів. Правове регулювання відносин щодо окремих видів інформаційних ресурсів.
Тема 2.	Концептуальна модель інтелектуальної мережі. Стандартизація в галузі інтелектуальних мереж. Концепція інтелектуальної мережі. Функція комутації послуг SSF.
Тема 3.	Послуги, що надаються інтелектуальною мережею. Послуги інтелектуальної мережі. Класифікація послуг та їх призначення.
Тема 4.	Створення системи управління інтелектуальною надбудовою. Загальні положення. Завдання та організаційна структура системи керування інтелектуальною надбудовою. Адміністративне керування потребує надання інформації про роботу усіх рівнів системи
Тема 5.	Захист інформації в сучасних інтелектуальних мережах. Характеристика захищених телекомунікаційних систем. Способи захисту інформації від перехоплення. Вимоги до радіоприймачів захищених систем. Забезпечення енергетичної скритності. Вимоги до шумових характеристик компонентів захищених систем.
Тема 6	Доступ до інформаційних ресурсів на основі бездротових мереж. Захисту інформації від несанкціонованого доступу в сучасних телекомунікаційних системах. Захист передавальної інформації за рахунок передавання сигнальних конструкцій. Принципи методів розширення спектру для забезпечення енергетичної прихованості. Метод псевдовипадкової перебудови робочої частоти.

Тема 7	Мережі широкосмугового бездротового доступу сімейства стандартів IEEE 802.16 (WiMAX). Захист інформації в широкосмугових системах зв'язку з розширенням спектру методом прямої послідовності (DSSS). Принцип роботи системи з кодовим розділенням каналів.

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-BP//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/.

1. 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

Щоп’ятниці у вересні-грудні 2024 року з 14^{20} до 15^{40} год., https://us02web.zoom.us/j/6197950058?pwd=YllCUkYwYlZYYU9rYmdsOUNTN3RlQT09 –

проф. В.В. Корчинський

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">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.</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

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 …….