СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи захисту інформації в комп’ютерних мережах

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	123 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Комп’ютерні мережі та інтернет
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-24 ОПП «Комп’ютерні мережі та інтернет»
Форма навчання	Денна

Викладач

Севастєєв Євген Олександрович
Seva.odessa@gmail.com

Старший викладач кафедри Кібербезпеки та технічного захисту інформації

Загальна інформація про дисципліну

Анотація до дисципліни

Дисципліна «Методи захисту інформації в комп’ютерних мережах» розглядає важливі аспекти забезпечення безпеки інформації в сучасних комп'ютерних мережах. Курс розроблений з метою підготовки студентів до розуміння та впровадження стратегій та технічних методів захисту даних у мережевому середовищі. В рамках цієї дисципліни розглядаються такі питання, як криптографія, мережеві загрози та інциденти, методи виявлення та реагування на інциденти, контроль доступу, безпека мережевого обладнання та програмного забезпечення, а також адміністрування безпеки мережі.

	Здобувачі вищої освіти отримають знання та практичні навички, необхідні для ефективного захисту інформації в мережевому середовищі, відповідно до сучасних стандартів і вимог безпеки. Після завершення курсу, вони зможуть визначати потенційні загрози, розробляти стратегії захисту і використовувати різноманітні інструменти для забезпечення конфіденційності, цілісності та доступності інформації в комп'ютерних мережах.
Мета дисципліни	– формування системних знань та розвиток умінь і навичок, що стосуються безпеки комп'ютерних мереж. Деякі можливі аспекти, які можуть бути включені у мету дисципліни, включають: – формування розуміння загальних принципів кібербезпеки, включаючи ідентифікацію потенційних загроз та ризиків; освоєння стратегій та технік захисту мереж і даних від несанкціонованого доступу, зламу та інших загроз; – ознайомлення з сучасними стандартами, протоколами та методами шифрування та аутентифікації в сучасних мережах; планування заходів безпеки та реагування на інциденти. –засвоєння основних принципів та практик забезпечення безпеки комп'ютерних мереж і формування готовності до викликів і загроз, пов'язаних з цією галуззю.
Компетентності, формуванню яких сприяє дисципліна	ЗК-3. Здатність застосовувати знання у практичних ситуаціях. СК-1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії СК-4. Здатністьзабезпечуватизахистінформації, щообробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізаціївстановленоїполітикиінформаційноїбезпеки СК-6. Здатність проєктувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення СК-9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи СК-10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації СК-12. Здатність Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання СК-16.Здатність створювати та обслуговувати стабільні, захищені, прогнозовані сегменти мережі Інтернет з високими показниками параметрів ефективності на основі використання новітніх технологій та протоколів
Результати навчання	ПРН-3. Знати новітні технології в галузі комп'ютерної інженерії. ПРН-18. Використовувати інформаційні технології для ефективного спілкування на професійному та соціальному рівнях. ПРН-22. Вміти застосовувати базові знання основних нормативно-правових актів та довідкових матеріалів, чинних стандартів і технічних умов, інструкцій та інших нормативно-розпорядчих документів у галузі комп'ютерної інженерії ПРН-25. Вміти проєктувати, впроваджувати, адмініструвати локальні, глобальні програмно-конфігуровані комп'ютерні мережі.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредити ЄКТС (120 годин). Для денної форми навчання: лекції – 16 годин, практичні заняття –14 годин, лабораторні заняття –14 годин,самостійна робота – 76 годин. Для заочної форми навчання: лекції – 6 годин, практичні заняття –4 години, лабораторні заняття – 4 години, самостійна робота –106 годин.

Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 5-му семестрі

Програма дисципліни

Тема 1.	*Поняття кібербезпеки: основні визначення в сфері захисту інформації* Вступ до дисципліни. Мета та задачі захисту інформації в корпоративних комп'ютерних мережах. Основні визначення, що використовуються в сфері захисту інформації
Тема 2.	*Керування доступом. Авторизація, Автентифікація, Аудит.* Загальні принципи керування доступом. Процес автентифікації – паролі, токени, біометрія як засіб автентифікації.Двофакторна автентифікація. Права користувачів в операційній системі та мережі. Засоби аудиту – логи та хешування. Протоколи авторизації. SSO. Моделі доступу.
Тема 3.	*Мережеві протоколи та атаки на них* Поняття physical layer security. Протоколи канального рівня та атаки на них. Методи захисту від атак на протоколи канального рівня.Захист інформації на мережевому та транспортному рівні. Протоколи безпеки рівня сеансу та додатків.
Тема 4.	*Архітектура захищених корпоративних мереж: проектування та розгортання безпечної інфраструктури* Елементи безпечної архітектури комп'ютерної мережі – Firewall, NAT, Proxy, Sandbox, VPN, BYOD та інші.
Тема 5.	*Фаєрвол для захисту периметру мережі в сучасних умовах* Захист мережевого периметру: перехоплення та контроль вхідного/вихідного трафіку.*NGFW.* Контроль додатків. Захист мережі від несанкціонованого доступу. Системи IDPS.
Тема 6.	*Конфіденційність даних в корпоративних радіомережах* Захист бездротових мереж: шифрування, ідентифікація та захист від несанкціонованого доступу
Тема 7.	*Хмарна інфраструктура та безпека в хмарі* Загальні підходи до безпеки інформації за межами периметру мережі. Архітектура Zero trust.

Список рекомендованих джерел

1. Лахно В.А., Василіу Є.В., Гладких В.М., Домрачев В.М., Сивкова Н.М. Методи та засоби захисту інформації [Навчальний посібник] /– К. : ЦП «Компринт» О.В., 2021. 444 с.
2. Northcutt, S. Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems. Pearson IT

Certification, 2021, 624 p.
3. Попов, С. М., та ін. Кібербезпека та захист інформації: навчальний посібник. Київ: КНЕУ, 2022, 342 с.
4. Литвиненко, В. В., Колесніков, А. О. Методичні рекомендації до вивчення дисципліни «Захист інформаційних систем». Харків: ХНУРЕ, 2021, 45 с.
5. Ткаченко, П. М., Дьяконов, І. М. Методичні рекомендації з виконання практичних завдань з кібербезпеки. Київ: ДУІКТ, 2023, 52 с.
6. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. International Organization for Standardization, 2022, 40 p.
7. ENISA. Good Practices for Secure Software Development Lifecycle. – European Union Agency for Cybersecurity, 2021, 58 p..
8. Олейніков А.М. Методи та засоби захисту інформації: навчальний посібник для студентів вищих навчальних закладів. Харків:НТМТ, 2014. 298с.

Інформація про консультації

Згідно графіку консультацій кафедри Кібербезпеки та технічного захисту інформації ДУІТЗ

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="11">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="10">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань, лабораторних та контрольних робіт) та за результати заліку/екзамену)</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, лабораторних 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 різні програмні засоби.
Умови зарахування пропущених занять: Зарахування пропущених практичних та лабораторних занять проводиться під час консультацій.
Інші умови: Навчально-методичні матеріали дисципліни розміщені на електронних платформах ДУІТЗ.