

## Силабус вибіркової дисципліни

| №   | Назва поля   | Детальний контент, коментарі   |
|-----|--|--|
| 1.  | Назва факультету   | Факультет інфокомунікацій  |
| 2.  | Рівень вищої освіти  | Master's, educational and scientific   |
| 3.  | Код і назва спеціальності                                      | 125 Кібербезпека   |
| 4.  | Тип і назва освітньої програми                                 | ОПП «Адміністративний менеджмент у сфері захисту інформації»   |
| 5.  | Код і назва дисципліни (інформація з ЦІСТ)                     | ААтБІСІ- Адміністрування, аудит та безпека інформаційних служб Internet  |
| 6.  | Кількість ЄКТС кредитів  | 6  |
| 7.  | Структура дисципліни (розподіл за видами та годинами навчання) | 30 г. – 15 лк, 4г.- 2ПЗ, 20 г. – 5 ЛБ, 12 г. – 6 конс, 2 г. – РГЗ, вид контролю: залік   |
| 8.  | Графік (терміни) вивчення дисципліни                           | 2-й рік, 3-й семестр   |
| 9.  | Передумови для навчання за дисципліною                         | Дисципліна базується на знаннях, отриманих в результаті вивчення дисциплін природничо-наукової підготовки (вища математика, фізика, алгоритмічні мови та програмування, комп'ютерні методи дослідження інформаційних процесів та систем, спеціальні розділи математики, основи теорії кіл, сигнали та процеси в інформаційно-комунікаційних системах, теорія інформації та кодування) з поглибленим вивченням дисциплін фахової підготовки (електроніка та мікросхемотехніка, алгоритмічні основи криптології, криптографічні системи та протоколи, WEB-програмування, комп'ютерні мережі, інформаційно-комунікаційні системи, бази даних та знань, архітектура комп'ютерних систем, мережеві операційні системи, прикладна криптологія, методи та засоби криптоаналізу, обчислювальна техніка, захист інформації в інформаційно-комунікаційних системах, технології та спеціальні розділи програмування |
| 10. | Анотація (зміст) дисципліни                                    | Мета вивчення дисципліни є вивчення архітектури протоколів веб-додатків, їх загальні вразливості та слабкі сторони, вразливості відкритих баз даних; аспекти безпеки, що використовують мови PHP, JavaScripts, SQL та ін; механізми веб-автентифікації та методи обходу автентифікації, помилки кодування додатків; існуючі вразливості та атаки на веб-ресурси, можливості їх практичного застосування та методи боротьби з ними на стадії проектування і в процесі експлуатації (OWASP – Open Web Application Security Project); шаблони дизайну для захищених веб-додатків; архітектуру безпеки, типову для веб-сервісів; тестування внутрішнього та зовнішнього проникнення, бездротове проникнення; інструменти безпеки.  |

|     |  |  |
|-----|--|--|
| 11. | Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання | За результатом вивчення дисципліни студенти повинні: знати: основи адміністрування, безпеки та аудиту сучасних інформаційних служб мережі інтернет (IIS), архітектуру протоколів веб-додатків, їх загальні вразливості та слабкі сторони, вразливості відкритих баз даних; аспекти безпеки, що використовують мови ASP, SQL та ін;   |
| 12. | Результати навчання здобувача вищої освіти   | За результатом вивчення дисципліни студенти повинні: вміти: проводити аналіз вразливостей та слабких сторін веб-програм; проводити тестування внутрішнього та зовнішнього проникнення; проводити дослідження з інформаційної безпеки клієнт-серверної системи; захистити веб-служби від кібер-атак на стадії проектування і в процесі експлуатації; захистити клієнтів та сервери на різних веб-платформах.  |
| 13. | Система оцінювання відповідно до кожного завдання для складання заліку/екзамену                    | <p>1. Відпрацювати та захистити лабораторні роботи.<br/> 2. Виконати контр. роботи на практичних заняттях.<br/> 3. Отримати за семестр не менше 60 балів.<br/> 4. Скласти екзамен.</p> <p>Оцінка за семестр <math>O_{\text{сем}} : (6-10) \times 4 \text{ лб} + (6-10) \times 4 \text{ пз} + (12-20) \times 1 \text{ РГЗ} = (60-100)</math> балів.<br/> Оцінка за екзамен (залік) <math>O_{\text{екз}} = (60-100)</math> балів.<br/> Екзамен комбінований у формі комп. тесту (20 завдань, тривалість 60 хв.).<br/> Підсумкова оцінка <math>O_{\text{д}}^{\text{екз}}</math> обчислюється за формулою:<br/> <math>O_{\text{д}}^{\text{екз}} = 0,6 \cdot O_{\text{сем}} + 0,4 \cdot O_{\text{екз}}</math>.</p>  |
| 14. | Якість освітнього процесу  | Оновлені робочі програми дисципліни – 2020-2021, 2021-2022 уч. р. Лабораторний практикум забезпечено сучасним апаратним та програмним забезпеченням.   |
| 15. | Методичне забезпечення   | <p>Базова література</p> <p>1. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.<br/> 2. Домарев В. В. Защита информации и безопасность компьютерных систем. К.: Диасофт, 1999. – 480 с.<br/> 3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.<br/> 4. Тардаскін М.Ф., Кононович В.Г. Технічний захист комерційної таємниці підприємства зв'язку: Навч. посібник/ За ред. М.В. Захарченка. – Одеса: ОНАЗ, 2002. – 76 с.<br/> 4. Банкет В. Л., Захарченко Н. В., Дырда А. В., Гулак Г. Н., Владишевский Б. С. Защита информации в системах телекоммуникации. Одесса.</p> <p>Допоміжна література</p> <p>1. Терейковский И. А. Безопасность программного обеспечения, созданного с использованием семейства технологий COM, DCOM, COM+ / И. А. Терейковский //</p> |

|     |   |   |
|-----|---|---|
|     |   | <p>Захист інформації. – 2006. – № 1. – С. 55–67.</p> <p>2.Терейковський І. А. Захищеність Web-серверів Apache та IIS / І. А. Терейковський // Проблеми програмування. – 2005. – № 2. – С. 42–51.</p> <p>3.Андреев А.Г. и др. Microsoft Windows XP. /Под общей ред. А.Н. Чекмарева. – СПб.: БХВ-Петербург, 2003. – 640 с.</p> <p>4.Марк Шпеник М., Следж Ор. Руководство администратора баз данных MS SQL Server.</p> <p>5.Хокинс С. Администрирование Web-сервера Apache и руководство по электронной коммерции. : Пер. с англ. М. : Издательский дом “Вильямс”, 2001. – 336 с.</p> <p>6.Домарев В. В. Защита информации и безопасность компьютерных систем. К.: Диасофт, 1999. – 480 с.</p> <p>7.Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.</p> <p>8. Навчально–методичний посібник “Інформаційні технології в економіці та бізнесі” / Укладач: А.В. Журавка, Харків: ХНУБА, 2016. –116 с.</p> <p>9.Навчально–методичний посібник “Економіко-математичне моделювання за допомогою електронних таблиць” /Укладач: Журавка А.В.– ХНУБА, 2018. – 132 с.</p> <p>10.Методичні вказівки до практичних занять з дисципліни «Information Security in information and Communication Systems» (Інформаційна безпека в інформаційних та комунікаційних системах) (англ. мовою) для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» [Електронне видання], Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2019. – 90 с.</p> <p>11.«DATABASE ADMINISTRATION AND SECURITY», guidelines for practics works on discipline for foreign students of the specialty «Cybersecurity», [Electronic resource], Composed by A.V.Zhuravka , Electronic Edition - Kharkiv: KNURE, 2020. – 62 p.</p> <p>12.Навчальний посібник з дисципліни «Адміністрування та безпека баз даних» для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2021. – 149 с.</p> <p>13.Навчальний посібник з дисципліни «Database Administration and Security» для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2022. – 139 с.</p> |
| 16. | Розробник силябусу (посада, ПІБ, ел. пошта) | А.В. Журавка, проф. каф. ІКІ, Ph.D.<br>E-mail: <a href="mailto:Andrii.Zhuravka@nure.ua">Andrii.Zhuravka@nure.ua</a>   |