| ЧЕРКАСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Богдана Хмельницького | **Силабус навчальної дисципліни «ОСНОВИ КРИПТОЛОГІЇ»** | | | |
|---|---|---|---|---|
| | Статус дисципліни: навчальна дисципліна вибіркового компонента | | | |
| Галузь знань | 12 Інформаційні технології<br>11 Математика та статистика | | | |
| Спеціальність | 126 «Інформаційні системи та технології»<br>113 «Прикладна математика» | | | |
| Освітня програма | Інтелектуальний аналіз даних<br>Прикладна математика | | | |
| Ступінь вищої освіти | Бакалавр | | | |
| Форма навчання | Денна | | | |
| Курс | 3-4 | | | |
| Семестр | 5-8 | | | |
| Обсяг дисципліни | Кредити | **4** | Години | **120** |
| Семестровий контроль | Залік | | | |
| Викладач | Дзюба В.А., к.т.н. | | | |
| Контактна інформація | viktoriya.dzyuba15@vu.cdu.edu.ua | | | |
| Кафедра | Кафедра прикладної математики та інформатики | | | |
| Навчально-науковий інститут / Факультет | ННІ інформаційних та освітніх технологій | | | |
| Мова викладання | Українська | | | |
| Предмет навчання (*Що буде вивчатися*) | - Основи симетричних та асиметричних криптосистем;<br>- шифрування та дешифрування даних;<br>- криптографічні хеш-функції;<br>- цифрові підписи;<br>- криптографічні протоколи;<br>- атаки на криптосистеми та методи захисту;<br>- квантова криптографія. | | | |
| Мета (*Чому це цікаво/потрібно вивчати*) | Криптологія є важливою частиною сучасних інформаційних технологій, оскільки забезпечує безпеку та конфіденційність даних, які відіграють ключову роль у всіх сферах життя — від особистої комунікації до глобальної економіки. | | | |
| Програмні результати (*Чому можна навчитися*) | У результаті вивчення навчальної дисципліни студенти зможуть:<br>- розуміти принципи сучасних криптосистем;<br>- використовувати криптографічні методи для захисту інформації;<br>- аналізувати безпеку систем та виявляти потенційні загрози;<br>- застосовувати криптографію в реальних проєктах та програмах;<br>- розробляти безпечні протоколи передачі даних. | | | |

<table>
<tr><td>Компетентності<br>(Як можна користуватися набутими знаннями і вміннями)</td><td colspan="2">Розробка та забезпечення безпеки інформаційних систем, робота у сфері кібербезпеки, розробка програмного забезпечення для захисту даних, консалтинг у питаннях інформаційної безпеки, аналітика та аудит систем безпеки.</td></tr>
<tr><td>Зміст дисципліни</td><td colspan="2">Змістовий модуль 1<br>Тема 1. Основи симетричних та асиметричних криптосистем.<br>Тема 2. Шифрування та дешифрування даних.<br>Тема 3. Криптографічні хеш-функції.<br>Тема 4. Цифрові підписи.<br><br>Змістовий модуль 2<br>Тема 5. Криптографічні протоколи.<br>Тема 6. Атаки на криптосистеми та методи захисту.<br>Тема 7. Квантова криптографія.</td></tr>
<tr><td rowspan="4">Розподіл годин</td><td>Лекційні</td><td>14</td></tr>
<tr><td>Практичні/семінарські</td><td>-</td></tr>
<tr><td>Лабораторні</td><td>26</td></tr>
<tr><td>Самостійна робота</td><td>80</td></tr>
<tr><td>Критерії оцінювання роботи студентів</td><td colspan="2">Завданням поточного контролю є систематична перевірка розуміння та засвоєння програмного матеріалу шляхом усного та письмового опитування, аналіз виконання завдань практичних занять, індивідуальної та самостійної роботи, умінь самостійно опрацьовувати навчальний матеріал, здатності публічно, письмово чи в електронному форматі представляти певний матеріал.<br><br>Критеріями оцінювання у ході поточного контролю є:<br>а) під час поточної аудиторної роботи на лекційних та практичних заняттях:<br>– активна участь у дискусіях та пропонованих формах роботи на лекційних та практичних заняттях;<br>– доповнення та запитання на лекційних та практичних заняттях.<br>б) при усних відповідях:<br>– повнота розкриття питання;<br>– логіка викладення, культура мовлення;<br>– впевненість, емоційність та аргументованість;<br>– використання основної та додаткової літератури (підручників, навчальних посібників, журналів, інших періодичних видань, інтернет-ресурсів тощо);</td></tr>
</table>

| | |
|---|---|
| | – аналітичні міркування, уміння робити порівняння, висновки.<br>в) при виконанні письмових завдань:<br>– повнота розкриття питання;<br>– цілісність, систематичність, логічна послідовність;<br>– підготовка матеріалу за допомогою комп'ютерної техніки, різних технічних засобів.<br>г) при виконанні завдань для самостійної та індивідуальної роботи:<br>– повнота виконання завдання;<br>– творчість та самостійність виконання.<br><br>Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни, який визначається до кожного завдання через якісні критерії і трансформується у мінімальну позитивну оцінку обраної для даної дисципліни шкали. Після завершення курсу використана шкала перенормовується у накопичувальну 100-бальну і ЄКТС (A, B, C, D, E, FX, F) шкали. |
| Інформаційне забезпечення (лінк на е-НМЗНД) | |
| Матеріально-технічне забезпечення | Аудиторія теоретичного навчання, комп’ютерний клас для виконання лабораторних робіт, ноутбук, проектор, навчальна та наукова література, презентаційні матеріали. |