

Міністерство освіти і науки України

Національний університет «Чернігівський колегіум» імені Т.Г.Шевченка



СИЛАБУС

навчальної дисципліни

Комп'ютерна безпека та захист інформаційних ресурсів

Загальна інформація

| | |
|---|--------------------|
| Компонент освітньо-професійної програми | <i>Нормативний</i> |
| Кількість кредитів ECTS | 3 |
| Мова навчання | <i>Українська</i> |
| Ступінь вищої освіти | |
| Галузь знань | |
| Спеціальність | |
| Освітньо-професійна програма | |

Мета навчальної дисципліни

Метою навчальної дисципліни «Комп'ютерна безпека та захист інформаційних ресурсів» є ознайомлення з основами кібербезпеки; оволодіння навичками застосування програмних засобів захисту даних в комп'ютерних системах застосування криптографічних та стеганографічних методів захисту даних.

Передумови вивчення дисципліни

Для результативного опанування знаннями, вміннями, навичками при вивченні даної дисципліни студент повинен мати базові знання з комп'ютерних мереж. Володіння комп'ютером, робота з операційною системою та вміння користуватися ресурсами мережі Інтернет.

Зміст дисципліни

Змістовий модуль 1. Апаратно-програмні засоби захисту даних в комп'ютерних системах

Тема 1. Інформація як найважливіший ресурс економіки. Персональні дані.

Типи корпоративних даних.

Тема 2. Основні поняття з галузі захисту інформаційних ресурсів.

Конфіденційність, цілісність та доступність.

Тема 3. Атаки. Методи проникнення (соціальна інженерія, злам пароля Wi-Fi, фішинг, використання вразливості)

Тема 4. Засоби пароліної ідентифікації та адміністрування

Тема 5. Архівування та резервне копіювання даних

Тема 6. Захист вмісту зовнішньої пам'яті. Захист вмісту запам'ятовуючих пристроїв від шкідливих програм.

Тема 7. Захист програмного забезпечення.

Тема 8. Поширені види мережових атак і способи захисту від них.

Змістовий модуль 2. Криптографічні та стеганографічні методи захисту даних

Тема 9. Основні поняття криптографії. Коротка історія криптографії.

Тема 10. Популярні алгоритми шифрування даних (симетричні: потокові, блокові; асиметричні).

Тема 11. Використання електронного підпису. Програмно-апаратні засоби шифрування даних.

Тема 12. Основні поняття стеганографії. Історія стеганографії. Стеганографічні методи і системи

Форми та методи навчання

Рекомендовані методи навчання: лекція, розповідь, бесіда, доповідь, ілюстрація та демонстрація, лабораторні та практичні роботи, самостійна робота, робота з джерелами інформації (література, Інтернет), дослідження, контроль та самоконтроль

Рекомендовані форми навчання: лекція, лабораторна робота, самостійна робота, практична робота, робота в групах, тестування.

Контроль навчальних досягнень

Форми та методи оцінювання:

Поточний контроль – експрес-опитування під час лекцій, відповіді на практичних заняттях, виконання та захист лабораторних робіт, усні доповіді, проходження комп'ютерного тестування.

Підсумковий контроль – залік.

Критерії оцінювання навчальних досягнень:

I рівень – низький. Студент не описує явища, не виявляє знання і розуміння основних положень теми.

II рівень – середній. Відповідь студента при відтворенні навчального матеріалу елементарна, зумовлюється початковими уявленнями про предмет вивчення.

III рівень – достатній. Відповідь повна, правильна, логічна, обґрунтована. Студент знає істотні ознаки понять, явищ, закономірностей, зв'язків між ними, а також самостійно застосовує знання в стандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки.

IV рівень – високий. Студент вільно володіє вивченим матеріалом, застосовує його на практиці в нестандартних ситуаціях, знання є глибокими, міцними.

Орієнтовний розподіл балів за видами робіт:

- 10% – усні опитування;
- 50% – лабораторні роботи;
- 15% – комп'ютерне тестування;
- 25% – підсумковий контроль.

Політика курсу

Учасники освітнього процесу керуються нормативними документами та відповідними Положеннями, затвердженими в НУЧК: розміщені на офіційному сайті університету у розділі «Публічна інформація про діяльність Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка» за посиланням: <http://chnpu.edu.ua/university/about/public-info>.

При вивченні дисципліни, виконанні лабораторних занять та проведенні форм контролю студенти зобов'язані дотримуватись принципів академічної доброчесності, зокрема не дозволяється списування, використання чужих завдань тощо.

Лабораторні роботи повинні бути захищені в терміни, що не перевищують двох тижнів після дати згідно плану занять.

Граничний термін захисту всіх лабораторних робіт та проходження всіх видів поточного контролю – не пізніше останнього дня навчання згідно розкладу.

Відпрацювання пропущених занять та перескладання всіх форм контролю може відбуватися щотижнево в день проведення консультацій за розкладом кафедри.

Матеріально-технічне забезпечення

Лекційна аудиторія з установленим мультимедійним обладнанням на базі комп'ютера IntelCeleronCPU G4900 та мультимедійного проектора ViewSonicPJD5122.

Клас ПЕОМ. 13 комп'ютерів на базі IntelCeleron CPU G4900 @ 2.90GHz. Використовується вільнопоширюване програмне забезпечення на базі ОС LinuxOpenSuse.

Домашній настільний ПК або ноутбук (при дистанційному навчанні) з ОС Windows або ОС Linux.

Комп'ютерна мережа, браузер.

Програми створення "віртуальної машини".

Програми створення комп'ютерних презентацій.

Прикладен програмне забезпечення (детально вказується в умовах лабораторних робіт).

Програмне забезпечення для підтримки дистанційного навчання (Zoom, Telegram, Viber).

Інформаційні ресурси

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. 272 с..
2. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
3. Що таке комп'ютерна безпека [Електронний ресурс] // Портал : arhiv-stateu.pp.ua. — Режим доступу \www/ URL: <http://arhiv-stateu.pp.ua/index.php?newsid=26223>. — Заголовок з екрана, доступ вільний, 27.03.2015
4. Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. 222 p.
5. Long Fred. Java coding guidelines : 75 recommendations for reliable and secure programs / Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda. - New York: Pearson Education Inc., 2014. - 277 p.
6. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.

Інформація про викладача

| | |
|---|--|
| Прізвище, ім'я, по батькові викладача | Костюченко Андрій Олександрович |
| Науковий ступінь, вчене звання, посада | к.п.н., старший викладач |
| Комунікація | Кафедра: інформатики і обчислювальної техніки E-mail: mail4lab@ukr.net Telegram: @KostiuchenkoA (канал: https://t.me/joinchat/AAAAAFSSWJz_hr98POUQaQ) Zoom: 3088166886 (Пароль 303) |
| Посилання на дисципліну в системах дистанційного навчання | https://moodle.chnpu.edu.ua/course/view.php?id=30 |
| Консультації | Відповідно до розкладу |