МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мережні інформаційні технології

першого рівня вищої освіти

КРОПИВНИЦЬКИЙ

1. Загальна інформація

Назва дисципліни	**Мережні інформаційні технології**
Розробники	**– Коваленко Анна Степанівна**, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету – **Коваленко Олександр Володимирович**, доктор технічних наук, професор, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету – **Марченко Костянтин Миколайович**, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Викладач	Лектор – **Коваленко Анна Степанівна**, кандидат технічних наук, доцент, https://scholar.google.com.ua/citations?user=jEfDXi0AAAAJ&hl=ru https://www.scopus.com/authid/detail.uri?authorId=57219410986 Асистент – **Марченко Костянтин Миколайович**, кандидат технічних наук, доцент, https://scholar.google.ru/citations?hl=ru&pli=1&user=fielzdsAAAAJ https://orcid.org/0000-0001-6269-5379
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20}
E-mail:	annasun911@gmail.com
Консультації	*очні* – відповідно до затвердженого графіку консультацій; *онлайн* – е-листування, у месенджері, вебінари на платформах Zoom, Discord

2. Анотація дисципліни

Навчальний курс «Мережні інформаційні технології» призначений для набуття теоретичних знань та практичних навичок ідентифікування, класифікування та опису рівня безпеки мережних комерційних чи наукових проектів. Отримання навиків пошуку та використанню мережного спеціалізованого системного інструментарію для вирішення проблем програмно-технічних систем з зазначенням можливих обмежень обраних технологій.

3. Мета і завдання дисципліни

Метою викладання навчальної дисципліни «Мережні інформаційні технології» є забезпечення здобувачів вищої освіти комплексом знань, умінь та навичок, необхідних для застосування в професійній діяльності у сфері ідентифікування, класифікування та опису роботи програмно-технічних засобів.

Завданням вивчення дисципліни є формування компетентностей:

– Вміння виявляти, ставити та вирішувати проблеми.

– 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

– Здатність вирішувати проблеми у галузі комп’ютерних та інформаційних технологій, визначати обмеження цих технологій.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення навчальної дисципліни студент буде:

Знати:

– Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

– Мати знання основ економіки та управління.

Вміти:

– Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

– Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

Набувати навичок автономії і відповідальності:

– Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Кількість кредитів / годин	4/120
Кількість змістових модулів	2
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю :	залік

7. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд. 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти. Застосовується матеріально-технічна база кафедри кібербезпеки та програмного забезпечення: мультимедійний проектор Epson EB-X41, спеціалізовані комп'ютерні лабораторії з персональними комп'ютерами Athlon II 215x2 (10 шт.), Athlon 2.4, (15 шт.), AMD Semprom LE-1150 (18 шт.), AMD Duron 1,2 GHz (15 шт.), OpenOffice версії 4.1.7

(ліцензія LGPL), Google Chrome версії 106.0.5249.62 (ліцензія EULA), Google Docs (free licence), ОС Kali Linux (free licence), Wireshark (free licence GNU), Mono C# (free licence - GNU), draw.io (free licence).

8. Політика дисципліни

Організація освітнього процесу. Учасники освітнього процесу повинні дотримуватися вимог Положення про організацію освітнього процесу ЦНТУ, Кодексу академічної доброчесності ЦНТУ, Положення про дотримання академічної доброчесності НПП та здобувачами вищої освіти, інших нормативних актів університету http://www.kntu.kr.ua/?view=univer&id=4.

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до:

– Положення про організацію освітнього процесу;
– Положення про організацію вивчення навчальних дисциплін вільного вибору;
– Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ;
– Кодексу академічної доброчесності ЦНТУ.

9. Навчально-методична карта дисципліни

Тема 1. Захист рівня операційної системи. Част. 1. Основи термінології. Підвищення безпеки системи.
Тема 2. Захист рівня операційної системи. Част. 2. Особливості підвищення безпеки Windows
Тема 3. Міжмережні екрани. Част. 1. Основи архітектури мереж. Приклади роботи з пакетами даних TCP/IP
Тема 4. Міжмережні екрани. Част. 2. Міжмережний екран з відкритими вихідними текстами на платформі Linux.
Тема 5. Сканери портів. Част. 1. Internet Assigned Numbers Authority (IANA). Огляд найпоширеніших протоколів.
Тема 6. Сканери портів. Част. 2. Огляд сканерів портів.
Тема 7. Сканери вразливостей. Част. 1. Теорія виявлення загроз в безпеці систем.
Тема 8. Сканери вразливостей. Част. 2. Огляд сканерів вразливостей.
Тема 9. Мережні аналізатори. Част. 1. Теорія та особливості застосування мережевих аналізаторів.
Тема 10. Мережні аналізатори. Част. 2. Огляд мережних аналізаторів.
Тема 11. Системи виявлення вторгнень. Част. 1. Теорія та приклади сигнатур мережевих систем виявлення вторгнень.
Тема 12. Системи виявлення вторгнень. Част. 2. Огляд систем виявлення вторгнень.

Тема 13. Засоби аналізу та керування. Част. 1. Основи використання системних, мережних та прикладних утиліт.

Тема 14. Засоби аналізу та керування. Част. 2. Програми моніторингу, конфігурації та аналізу системи.

Лабораторна робота 1. Розробка поштового клієнта. Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 2. Розробка сканера TCP/UDP. Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 3. Розробка сканера безпеки. Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 4. Розробка програмного забезпечення що реєструє дії користувача (KEYLOGGER). Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 5. Вивчення механізму аналізу перехоплених пакетів протоколу TCP/IP. Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 6. Вивчення механізму розподілених атак типу «відмова в обслуговуванні» (DoS/DDoS). Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

Лабораторна робота 7. Вивчення механізму фішинг запитів. Створення технічного завдання. Розробка мережного програмного забезпечення. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.

10. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік.

Контроль знань і умінь здобувачів (поточний і підсумковий) здійснюється згідно з кредитною трансферно-накопичувальною системою організації освітнього процесу в ЦНТУ. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається із рейтингу з поточної навчальної роботи впродовж семестру, для оцінювання якої призначається 100 балів (по 50 балів за кожен змістовний модуль).

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті.

При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

11. Рекомендована література й джерела

Базова

1. Коваленко А.С., Коваленко О.В., Смирнов О.А., Смирнов С.А. Технологія тестування DOM XSS вразливості. Scientific & practical cyber security journal (SPCSJ) Volume 1. Issue 1. P. 38-45 **Georgia**. Tbilisi. Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667. Режим доступу: https://journal.scsa.ge/wp-content/uploads/2018/12/8-dom-xss-testing-technology-vulnerabilities.pdf (**Закордонне фахове видання**)
2. A. Kovalenko, O. Kovalenko, O. Smirnov, S. Smirnov, V. Vialkova. The mathematical model of the testing technology for DOM XSS vulnerabilities. Scientific & practical cyber security journal (SPCSJ) Vol 2 Issue 1, 22-28 pp. Georgia. Tbilisi: SCSA – 2018. Режим доступу: https://journal.scsa.ge/ru/papers/the-mathematical-model-of-the-testing-technology-for-dom-xss-vulnerabilities-3/ (**Закордонне фахове видання**)
3. Коваленко А.С., Смірнова Т.В., Буравченко К.О., Щербань А.В., Багдасарян Е.К., «Проектування та оптимізація структурованих кабельних систем для автоматизації виробничих процесів підприємства» Сучасні інформаційні системи. 2022. Т. 6, № 1. С. 129-133. Режим доступу: http://ais.khpi.edu.ua/article/view/254256/251522 **(Фахове видання. Категорія «Б»)**
4. Смірнова Т.В., Янков М.О., Грудік В.В., Горбов В.О., Коваленко А.С. «Планування радіопокриття та моделювання поширення радіосигналів мобільних мереж 5G для автоматизації виробничих процесів». Електронне моделювання, № 3, т. 44. С. 113-122. 2022. Режим доступу: https://www.emodel.org.ua/uk/archive-ukr/2022/44-3-u/c-113-122 **(Фахове видання. Категорія «Б»)**
5. Коваленко А.С., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов О.А., Смірнов С.А., Основи безпеки в комп'ютерних мережах, **Навчальний посібник** – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

Допоміжна

6. Vinit Jain. Wireshark Fundamentals. Apress Media. 2022. 267 c.
7. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 c.
8. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 c.
9. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 c.
10. Matt Walker. Certified Ethical Hacker Practice Exams. McGraw Hill. 2022. 352 c.
11. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 c.
12. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 c.
13. Nishant Bhajaria. Data Privacy. Manning. 2022. 805 c.
14. Joshua S. Ponelat, Lukas L. Rosenstock. Designing APIs with Swagger and OpenAPI. Manning Publications. 2022. 426 c.
15. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 c.
16. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 c.
17. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 c.
18. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 c.
19. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 c.

Методичне забезпечення

20. Коваленко А.С., Коваленко О.В., Марченко К.М. «Мережні інформаційні технології». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 60 с.
21. Коваленко А.С., Коваленко О.В., Марченко К.М. «Мережні інформаційні технології». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 60 с.

Інформаційні ресурси

22. Онлайн-курси UDEMY. – URL: https://www.udemy.com/ –платформа онлайн-курсів різних IT тематик.
23. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/ – українська платформа безкоштовних онлайн-курсів
24. Онлайн-курси Coursera. – URL: https://www.coursera.org –платформа онлайн-курсів різних IT тематик.
25. https://habr.com – колективний блог з новинами та аналітичними статтями про інформаційні технології та програмування.
26. http://stackoverflow.com/ – система питань і відповідей для професійних програмістів та новачків у програмуванні.
27. https://dou.ua/ – український веб-сайт з елементами колективного блогу, створений для розповсюдження новин, аналітичних статей та свіжої інформації пов'язаної із інформаційними технологіями.
28. https://www.google.com/ – основна пошукова платформа.
29. https://www.youtube.com – Відеохостинг, що надає користувачам послуги зберігання, доставки та показу відео. На платформі розміщено багато курсів IT спрямованості.
30. https://biblprog.org.ua/ua/programming/ – каталог безкоштовних середовищ розроблення ПЗ.