СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ»

Компонента освітньої програми – *вибіркова* (*3 кредити*)

Освітньо-наукова програма	Комп'ютерна інженерія
Спеціальність	F7 Комп'ютерна інженерія
Галузь знань	F Інформаційні технології
Рівень вищої освіти	Другий (магістерський)
Мова навчання	Українська
Профайл викладача	Танасюк Ю. В., доцент кафедри комп'ютерних систем та мереж, канд. фіз.-мат. наук, доцент (https://csn.chnu.edu.ua/employees/tanasyuk-yuliya-volodymyrivna/)
Контактний тел.	+(38) 0372 50 94 32
E-mail:	y.tanasyuk@chnu.edu.ua
Сторінка курсу	*https://www.netacad.com/courses/network-defense?courseLang=uk-UA*
Консультації	*Очні консультації*: за попередньою домовленістю. *Онлайн-консультації*: згідно з погодженим графіком.

АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Технології безпеки комп'ютерних мереж» ґрунтується на матеріалах професійно орієнтованого курсу **Network Defense** Cisco Networking Academy® та спрямована на формування базових знань і практичних навичок у сфері захисту комп'ютерних систем і мереж. Дисципліна охоплює принципи мережної безпеки, методи контролю доступу, міжмережні екрани, хмарну безпеку, криптографічні механізми, моніторинг мережної безпеки, аналіз журналів і сповіщень про події безпеки. Особлива увага приділяється практичному застосуванню засобів захисту, налаштуванню політик доступу та фільтрації трафіку, аналізу даних і виявленню потенційних загроз.

Мета навчальної дисципліни полягає у формуванні у студентів системного розуміння принципів забезпечення безпеки комп'ютерних систем і мереж та набутті практичних навичок застосування сучасних механізмів захисту, контролю доступу, фільтрації трафіку, криптографії, хмарної безпеки та моніторингу подій безпеки.

НАВЧАЛЬНИЙ КОНТЕНТ ОСВІТНЬОГО КОМПОНЕНТА

МОДУЛЬ 1. Багатошаровий захист розподілених систем та мереж	
Тема 1	Аспекти захисту комп'ютерних систем та мереж.
Тема 2	Методи та засоби контролю доступу. Технології брандмауерів і зональні політики безпеки.
МОДУЛЬ 2. Аналіз даних для виявлення потенційних загроз	
Тема 1	Безпека хмарних сховищ
Тема 2	Моніторинг безпеки. Системи журналювання даних та оповіщення про загрози.

ОСВІТНІ ТЕХНОЛОГІЇ, ФОРМИ ТА МЕТОДИ МЕТОДИ НАВЧАННЯ

У рамках дисципліни передбачено проведення лекцій та лабораторних занять, виконання завдань із застосуванням комп'ютерної та телекомунікаційної техніки, а також програмного забезпечення з відкритим кодом та онлайн-доступом. Самостійна робота, пов'язана з опрацюванням матеріалів лекцій та літературних джерел за відповідною тематикою, супроводжується формуванням напрацювань для подання та обґрунтування отриманих результатів виконання лабораторних завдань, підготовкою до контрольних робіт та тестів. Також під час проведення занять студенти залучені до виконання робіт на реальному мережному обладнанні та у симуляторі, беруть участь у обговореннях у малих групах, проєктному навчанні. У окремих випадках під час проведення занять використовуються мультимедійні засоби Google Meet і Cisco Webex і освітні платформи Moodle та netacad.com.

У межах дисципліни передбачено можливість використання результатів навчання, здобутих студентами під час проходження професійно-орієнтованих онлайн-курсів Cisco Networking Academy (NetAcad), зокрема Network Defense (українською мовою). Результати навчання, отримані поза межами формальної освітньої програми, можуть бути визнані відповідно до встановленого в університеті порядку за умови підтвердження їх успішного здобуття та відповідності програмним результатам навчання дисципліни.

Методи навчання: словесні (лекція, пояснення, дискусія, навчальна бесіда); наочні (демонстрація, ілюстрація, аналіз схем і моделей мережної інфраструктури); практичні (лабораторні роботи, практичні завдання, моделювання мережних атак і засобів захисту, аналіз мережного трафіку); проблемно-орієнтоване навчання; проєктне навчання; кейс-метод; дослідницький метод; кооперативне навчання; метод взаємного навчання й оцінювання.

ФОРМИ Й МЕТОДИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ

***Поточний контроль*:** усні та письмові відповіді студентів; подання та аргументований захист результатів розв'язку практичних завдань у рамках колективного обговорення; виконання завдань проміжних та підсумкових контрольних робіт; результати складання тестів.

Підсумковий контроль – залік.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання програмних результатів навчання здобувачів освіти здійснюється за шкалою європейської кредитно-трансферної системи (ECTS).

Критерієм успішного оцінювання є досягнення здобувачем вищої освіти мінімальних порогових рівнів (балів) за кожним запланованим результатом навчання.

ПОЛІТИКА ЩОДО АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ЧНУ:

– «Кодекс академічної доброчесності та етики Чернівецького національного університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/kodeks-akademichnoi-dobrochesnosti-ta-etyky-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/

– «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-

zapobihannia-akademichnomu-plahiatu-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/

– «Політика використання штучного інтелекту в Чернівецькому національному університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polityka-vykorystannia-shtuchnoho-intelektu-v-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha-zi-zminamy-zatverdzhenymy-vchenoiu-radoiu-chnu-imeni-yuriia-fedkovycha/

ВИКОРИСТАННЯ ЗДОБУВАЧАМИ ОСВІТИ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) ПІД ЧАС ВИКОНАННЯ НАВЧАЛЬНИХ ЗАВДАНЬ:

– **допускається** за умови дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої роботи, а у разі використання ШІ зобов'язаний зазначити факт і спосіб його застосування);

– **не допускається** використання ШІ як заміни самостійного виконання завдань або з метою порушення вимог академічної доброчесності;

– **додаткові обмеження чи вимоги** щодо використання ШІ можуть визначатися викладачем в освітньому процесі для конкретних видів навчальної діяльності відповідно до особливостей дисципліни.

ІНФОРМАЦІЙНІ РЕСУРСИ

https://csn.chnu.edu.ua/students/repozytarij-kafedry-ksm/
https://moodle.chnu.edu.ua
https://www.netacad.com/career-paths/cybersecurity?courseLang=uk-UA
https://www.netacad.com/courses/network-defense?courseLang=uk-UA