Назва курсу	**«Кібербезпека інформаційних і комп'ютерних систем»**
Викладач (-і)	Яцків Василь Васильович
Профайл викладача (-ів)	http://www.tneu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	**v.yatskiv(@)tneu.edu.ua**
Сторінка курсу в moodle	https://moodle.tneu.edu.ua
Консультації	Очні консультації: понеділок: 14-00, ауд. 6501. Онлайн- консультації: у viber групі курсу кожного дня з 14 -00 до 18-00.

1. Анотація до курсу. Розкриття кіберзлочинів, кібер-шпигунства та інших загроз цілісності мереж та систем - це нова захоплююча область, яка охоплює всі галузі. Курс зосереджений на тому, як слідкувати, виявляти та реагувати на загрози кібербезпеки. Крім того, охоплює криптографію, аналіз безпеки на основі хостів, моніторинг безпеки, комп'ютерну криміналістику, методи атак та обробку випадків порушення безпеки.

2. Пререквізити.

Раніше вивчені дисципліни необхідні для освоєння курсу: методологія наукових досліджень, інформаційні технології, математичне моделювання та обчислювальні методи.

Постреквізити. Дисципліни, які будуть використовувати результати навчання даного курсу: підготовка дисертаційної роботи.

3. Мета та цілі курсу.

Метою курсу "Кібербезпека інформаційних і комп'ютерних систем" є отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп'ютерних системах та мережах і усунення проблем безпеки шляхом розробки та впровадження захисних заходів.

Результати навчання:

В результаті вивчення дисципліни аспірант повинен:

Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у інженерії програмного забезпечення та дотичних міждисциплінарних напрямах.

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**доктор філософії**
Спеціальність	**121** **Інженерія програмного забезпечення**
Курс (рік навчання)	**1**
Семестр	**2**
Рік викладання	**2020**
Формат курсу	Очний (offline)
Нормативна \ вибіркова	**нормативна**
Загальна кількість год/ кредитів	**150/5**
Лекції, год.	**30**
Лабораторні, год	**15**
Самостійна робота, год.	**105**

5. Перелік тем

Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. Кіберпростір і кібербезпека - головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти.

Тема 2. Класифікація атак за рівнями ієрархічної моделі OSI. Атаки на фізичному рівні. Атаки на канальному рівні. Атаки на мережевому рівні. Атаки на транспортному рівні. Атаки на рівні додатків.

Тема 3. Атаки на бездротові пристрої. Атаки на Wi-Fi. Атаки на Bluetooth. Атаки на сенсори мобільних пристроїв.

Тема 4. Вразливості. Основні типи вразливостей. Приклади вразливостей. Захист від вразливостей.

Тема 5. Атаки в віртуальному середовищі. Технології віртуалізації. Мережеві загрози у віртуальному середовищі. Захист віртуального середовища. Security Code vGate. Віртуальні загрози майбутнього.

Тема 6. Безпека хмарних технологій. Принцип хмари. Безпека хмарних систем. Методи шифрування в хмарних сервісах.

Тема 7. Методи та засоби захисту інформації. Організація захисту від вірусів. Міжмережеві екрани. Засоби запобігання витокам інформації. Засоби шифрування. Одноразова аутентифікація. Honeypot - пастка для хакера.

Тема 8. Стандарти та нормативна документація в галузі кібербезпеки. Політики безпеки. Регламент управління інцидентами.

Тема 9. Безпека Інтернет речей. Концепція Інтернет речей (IoT). Архітектура IoT. Моделі зв'язку IoT.

Тема 10. Основи технології блокчейн та приклади застосування. Принцип технології блокчейн. Структура блоку та дерево Меркле. Криптографія в блокчейн

Література: 12, 13

Тема 11. Алгоритми консенсусу в технології блокчейн. Алгоритм доказу виконання роботи (Proof-of-Work). Алгоритм підтвердження частки (Proof-of-Stake). Альтернативні алгоритми консенсусу.

Література: 12, 13

Тема 12. Безпека Інтернет речей на основі технології блокчейн. Інтернет речей на основі технології блокчейн. Переваги інтеграції блокчейну з IoT. Основні виклики для блокейну в IoT. Блокчейн рішення для безпеки Інтернет речей.

6. Рекомендовані джерела інформації

1. CCNA Cybersecurity Operations. Курс Мережевої академії Cisco. Електронний ресурс. Режим доступу: https://www.netacad.com/courses/security/ccna-cybersecurity-operations

2. Santos, Omar, Joseph Muniz, and Stefano De Crescenzo. CCNA Cyber Ops SECFND# 210-250 Official Cert Guide. Cisco Press, 2017.

3. Dulaney, Emmett, and Chuck Easttom. CompTIA Security+ Study Guide: Exam SY0-501. John Wiley & Sons, 2017.

4. Gregg, Michael. Certified Ethical Hacker (CEH) Version 9 Cert Guide. Pearson IT Certification, 2017.

5. Santos, Omar, and John Stuppi. CCNA Security 210-260 Official Cert Guide: CCNA Sec 210-260 OCG. Cisco Press, 2015.

6. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок. - К.: НАУ, 2013.- 432 с.

7. Бирюков А. А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012. - 474 с.

8. ISACA. Впровадження європейської кібербезпеки: настанови з управління ризиками, США, 2014 р.

9. Dotson C. Practical Cloud Security A Guide for Secure Design and Deployment. O'Reilly Media; 1 edition, 2019. - 196.

10. Кузнецов О.О. Стеганографія: навч.посібн. / О.О.Кузнецов, С.П.Євсеєв, О.Г.Король. – Х.:Вид.ХНЕУ, 2011. - 232 с.

11. Ли П. Архитектура интернета вещей / пер. с анг. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 454 с.

12. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. -547 с.

13. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security of IoT: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, Ternopil National Economic University, 2019. – 98 p.

7. Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни **"Кібербезпека інформаційних і комп'ютерних систем"** визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту.

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовольняє, може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання:

За шкалою ТНЕУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

8. Навчальні ресурси

№	Найменування
1.	**Обладнання:** проектор, комп'ютери з доступом до мережі Інтернет.
2.	**Програмне забезпечення:** VM VirtualBox, Образи віртуальних машин з заданими вразливостями.

9. Політики курсу.

Академічна доброчесність. **Дотримання академічної доброчесності аспірантами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.