СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Методологічні засади кібербезпеки
Мова викладання	українська
Викладач (-і)	М.Є. Шелест професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
Профайл викладача (-ів)	0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. Анотація курсу -

Настав новий етап у розвитку інформаційного обміну, який характеризується інтенсивним впровадженням сучасних інформаційних технологій, широким розповсюдженням локальних, корпоративних та глобальних мереж у всіх сферах життя цивілізованої держави, що створює нові можливості та якість обміну інформацією. У зв'язку з цим проблеми інформаційної безпеки набувають першорядного значення.

Метою вивчення дисциплін є формування професійної компетентності на основі системи теоретико-методологічних знань та спеціальних навичок у галузі інформаційної безпеки та їх використання у професійній діяльності майбутнього фахівця.

Змістовий модуль 1. Проблеми розвитку теорії і практики забезпечення інформаційної безпеки.

Тема 1. Основні поняття і визначення в області інформаційної безпеки.

Терміни, що визначають наукову складову кібербезпеки. Терміни, що визначають предметну складову кібербезпеки. Терміни, що визначають характер діяльності по забезпеченню інформаційної безпеки.

Тема 2. Визначення кібербезпеки у світлі інформаційних проблем сучасного суспільства.

Основні складові кібербезпеки. Значення кібербезпеки для суб’єктів інформаційних відносин. Складові національних інтересів України в інформаційній сфері. Міжнародна співпраця в галузі кібербезпеки: проблеми та перспективи.

Змістовий модуль 2. Загальний зміст захисту інформації.

Тема 3. Поняття і сутність кібербезпеки.

Основні цілі захисту інформації. Концептуальна модель кібербезпеки. Інформація як об’єкт права власності. Загрози кібербезпеки, модель гіпотетичного порушника інформаційної безпеки.

Тема 4. Системне забезпечення захисту інформації.

Основні принципи побудови системи захисту. Методи кібербезпеки: мінімізація збитку від аварій та стихійних лих, дублювання інформації,

підвищення надійності інформаційної системи, створення відмовостійкої системи, оптимізація взаємодії користувачів і обслуговуючого персоналу, методи і заходи захисту інформації від шпигунства та диверсій, та ін. Моделі захисту інформації.

2. Мета та цілі курсу -

Метою дисципліни «Методологічні засади кібербезпеки» є формування професійної компетентності на основі системи теоретичних і методологічних знань і спеціальних умінь в області інформаційної безпеки і їх використання у професійній діяльності майбутнього фахівця.

Завданнями вивчення навчальної дисципліни є:

- навчити організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- отримати практичні навички використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності
- сформувати відповідні компетентності щоб аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- набути вмінь впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- отримати відповідні компетентності щоб забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- ознайомити з принципами використання цих програмно-апаратних та технічних комплексів захисту інформаційних ресурсів;
- навчити вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки та задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- отримати необхідні навички для забезпечення належного функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 4. Здатність розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

3. Результати навчання –

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 6. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою;

ПРН 9. розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

У результаті вивчення навчальної дисципліни студент повинен:

Знати:

- проблеми розвитку теорії та практики забезпечення інформаційної безпеки;
- ключові компоненти інформаційної безпеки;
- цінність інформаційної безпеки для суб'єктів інформаційних відносин;
- загрози інформаційній безпеці;
- гіпотетична модель захисту інформації.

Вміти:

- виявити загрози інформаційній безпеці та проводити аналіз ризиків на підприємстві;
- мінімізовувати збитки від аварій та стихійних лих;
- підвищити надійність інформаційної системи;
- оптимізовувати взаємодію користувачів та персоналу;
- використовувати сучасні моделі захисту інформації.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	16

практичні	14
самостійна робота (контрольна робота)	90

5. Пререквізити -

Вивчення дисципліни «Методичні засади кібербезпеки» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Вища математика», «Спеціальні глави математики», «Основи програмування», «Основи криптографічного захисту інформації».

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• лабораторні роботи : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•КР: 20% семестрової оцінки;

• залік: 40% семестрової оцінки.

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

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

8. Рекомендована література

Базова

1. О.В.Вербіцький. Вступ до криптології. Видавництво НТЛ., Львів, 2008, с.248.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, - М.: Радио и связь, 2007. -328 с.

3. Баричев С.Г., Серов Р.Е. Основы современной криптографии. – М.: Радио и связь, 2015. – 152 с.
4. Молдовян А.А., Молдовян В.А., Советов В.Я. Криптография. – Серия “Учебники для вузов. Специальная литература”. – Спб.: Издательство “Лань”, 2006. – 224 с.
5. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
6. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнійчук, 2011. – 152 с.
7. А.О.Антонюк. Основи захисту інформації в автоматизованих системах. – К.: КМ Академія, 2006. – 244 с.
8. А.Ю.Щеглов. Защита компьютерной информации от несанкционированного доступа. НиТ:Санкт-Петербург, 2004.
9. Hoffstein J. An Introduction to Mathematical Cryptography / J. Hoffstein, J. Pipher, J. Silverman. - Springer Science+Business Media, LLC, 2008. – 524 p.
10. Jeffrey H. An Introduction to Mathematical Cryptography / H. Jeffrey, P. Jill, H. Joseph. – Berlin: Springer, 2008. – 540 p.
11. Ян С. Криптоанализ RSA / С. Ян. — Ижевск: РХД. 2011. — 312 с.
12. Srivastava A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem / A. Srivastava, A. Mathur // International Journal of Scientific and Research Publications. – 2013. – Vol. 3 (6). – P. 1-4.
13. Hayder R.H. H-Rabim Cryptosystem / R.H. Hayder // Journal of Mathematics and Statistics. - 2014. – Vol. 10 (3). – P. 304-308.
14. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП. – 2001. – 254с.

Допоміжна

Домарев В.В.. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. 688 с.

Казарин О.В. Теория и практика защиты программ. М.: МГУЛ, 2003. 450 с.

Фергюсон Нильс, Шнайер Брюс. Практическая криптография / Н.Н. Селина (пер.с англ.). - М.; СПб.; К. : Диалектика, 2015. - 421с.

Харин Юрий Семенович, Берник Василий Иванович, Матвеев Геннадий Васильевич, Агиевич Сергей Валерьевич. Математические и компьютерные основы криптологии : Учеб. пособие для студ. мат. и инж.-техн. спец. вузов - Минск : ООО "Новое знание", 2013. - 382с.

Інформаційні ресурси

Новітні теоретичні та практичні дані та матеріали? що стосуються теорії та практики захисту інформації рекомендується відслідковувати засобом звертання до наступних сайтів.

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org

4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca
12. http://www.financialcryptography.com
13. http://www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. http://www.cryptonessie.org
16. http://www.cryptography.ru
17. http://www.osti.gov/eprints
18. http://www.intel.com
19. http://www.msdn.com
20. http://www.ph4s.ru/book_kripto.html