

1. Загальна інформація	
Назва дисципліни	<i>Основи кібербезпеки вибіркова</i>
Рівень вищої освіти	<i>Перший (бакалаврський) рівень</i>
Викладач	<i>Неласа Ганна Вікторівна, к.т.н., доцент, професор каф. ЗІ</i>
Контактна інформація викладача	<i>5-97</i>
Час і місце проведення навчальної дисципліни	<i>Предметна аудиторія кафедри ІТЕЗ</i>
Обсяг дисципліни	<i>Кількість годин - 90, кредитів - 3, розподіл годин (лекції-14, лабораторні-14, самостійна робота - 60, інші - 2), вид контролю – залік(5 семестр)</i>
Консультації	<i>Згідно з графіком консультацій</i>
2. Пререквізити і постреквізити навчальної дисципліни	
<p>Дисципліна "Основи кібербезпеки" базується на знаннях з дисциплін: "Вища математика", "Інформаційні технології", "Програмування".</p> <p>Дисципліни, для вивчення яких є обов'язковими знання, здобуті при вивченні цієї дисципліни: "Основи конструювання мехатронних систем", "Основи конструювання робототехнічних систем", "Основи конструювання електронних приладів", "Архітектура комп'ютерних систем та мереж", "Програмування для мобільних платформ", "Програмування систем на ПЛІС", "Web-дизайн", "Хмарні технології", "Інтернет речі в побуті", "Промисловий інтернет речей", "SmartCity", "Безпілотні технології", "Комп'ютерно-інтегровані технології на виробництві", "Діагностика та надійність комп'ютерних систем".</p>	
3. Характеристика навчальної дисципліни	
<p>Вивчення даної навчальної дисципліни формує у студента знання принципів, стандартів та засобів захисту інформації при проектуванні мехатронних і робототехнічних систем; надає практичні навички використання сучасних методів та засобів для забезпечення конфіденційного обміну, обробки та зберігання інформації.</p> <p>При вивченні даної дисципліни студент отримує:</p> <p><i>Загальні компетентності:</i></p> <p>K01. Здатність застосовувати знання у практичних ситуаціях K02. Здатність спілкуватися державною мовою як усно, так і письмово K03. Здатність спілкуватися іноземною мовою K04. Навички використання інформаційних і комунікаційних технологій K05. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел K06. Навички здійснення безпечної діяльності</p> <p><i>Фахові компетентності:</i></p> <p>K11. Здатність застосовувати знання математики, в обсязі, необхідному для використання математичних методів для аналізу і синтезу систем автоматизації. K15. Здатність обґрунтовувати вибір технічних засобів автоматизації на основі розуміння принципів їх роботи аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації і експлуатаційних умов; налагоджувати технічні засоби автоматизації та системи керування. K18. Здатність проектування систем автоматизації з врахуванням вимог відповідних нормативно-правових документів та міжнародних стандартів.</p> <p><i>Результати навчання:</i></p> <p>ПР01. Знати лінійну та векторну алгебру, диференціальне та інтегральне числення, функції багатьох змінних, функціональні ряди, диференціальні рівняння для функції однієї та багатьох змінних, операційне числення, теорію функції комплексної змінної, теорію ймовірностей та математичну статистику, теорію випадкових процесів в обсязі, необхідному для користування математичним апаратом та методами у галузі автоматизації. ПР03. Вміти застосовувати сучасні інформаційні технології та мати навички розробляти алгоритми та комп'ютерні програми з використанням мов високого рівня та технологій об'єктно-орієнтованого програмування, створювати бази даних та</p>	

використовувати інтернет-ресурси.

ПР04. Розуміти суть процесів, що відбуваються в об'єктах автоматизації (за галузями діяльності) та вміти проводити аналіз об'єктів автоматизації і обґрунтовувати вибір структури, алгоритмів та схем керування ними на основі результатів дослідження їх властивостей.

ПР08. Знати принципи роботи технічних засобів автоматизації та вміти обґрунтувати їх вибір на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації та експлуатаційних умов; мати навички налагодження технічних засобів автоматизації та систем керування.

4. Мета вивчення навчальної дисципліни

Мета вивчення дисципліни полягає у формуванні у студентів загальних методологічних основ і практичних навичок в галузі захисту інформації, вміння орієнтуватися в сучасних нормативних документах та стандартах в цій галузі, навичок з вибору відповідних криптографічних схем при проектуванні електронних засобів.

5. Завдання вивчення дисципліни

У результаті вивчення навчальної дисципліни студент повинен

знати:

- правові засади та сучасні стандарти України в галузі кібербезпеки;
- базові криптографічні примітиви для побудови системи захисту;
- загальні принципи захисту інформації в операційних системах та базах даних;

вміти:

- розробляти стратегію захисту критичної інфраструктури;
- використовувати криптографічні примітиви;
- організовувати захист від мережевих атак.

6. Зміст навчальної дисципліни

Дисципліна складається з лекційного курсу, лабораторних робіт та самостійної роботи.

У лекційному курсі з 7 тематичних лекцій розглядаються питання забезпечення захисту конфіденційної інформації при її передачі, обробці та зберіганні, сучасні стандарти криптографічного захисту, стеганографічні методи.

Для отримання базових практичних навичок з відповідних тем виконуються 7 лабораторних робіт, присвячених отриманню практичних навичок роботи з сучасними методами та засобами захисту інформації:

1. Симетричні блокові шифри
2. Симетричні поточні шифри
3. Асиметрична криптографія. Дискретний логарифм.
4. Сучасні протоколи автентифікації. Двофакторна автентифікація.
5. Шифрування та цифровий підпис в OpenSSL
6. Вейвлет-аналіз трафіку комп'ютерної мережі
7. Принципи стеганографії. Цифрові водяні знаки.

Самостійна робота полягає у самостійному вивченні окремих розділів лекційного курсу та виконанні індивідуального завдання.

Студенти заочної форми навчання виконують контрольну роботу.

7. План вивчення навчальної дисципліни

№ тижня	Назва теми	Форми організації навчання	Кількість годин
1.	Тема 1. Вступ до кібербезпеки	лекція	2
2.	Лабораторна робота 1. Симетричні блокові шифри	лаб. робота	2
3.	Тема 2. Законодавство в галузі кібербезпеки	лекція	2
4.	Лабораторна робота 2. Симетричні поточні шифри	лаб. робота	2
5.	Тема 3. Основи криптології та криптоаналізу	лекція	2

6.	Лабораторна робота 3. Асиметрична криптографія. Дискретний логарифм.	лаб. робота	2
7.	Тема 4. Криптографічні протоколи	лекція	2
8.	Лабораторна робота 4. Сучасні протоколи автентифікації. Двофакторна автентифікація	лаб. робота	2
9.	Тема 5. Інфраструктура відкритих ключів	лекція	2
10.	Лабораторна робота 5. Шифрування та цифровий підпис в OpenSSL	лаб. робота	2
11.	Тема 6. Методи виявлення атак	лекція	2
12.	Лабораторна робота 6. Вейвлет-аналіз трафіку комп'ютерної мережі	лаб. робота	2
13.	Тема 7. Стеганографічний захист	лекція	2
14.	Лабораторна робота 7. Принципи стеганографії. Цифрові водяні знаки.	лаб. робота	2

8. Самостійна робота

Самостійна робота виконується за дистанційною формою і складається з 10 тем для теоретичного вивчення та виконання індивідуального завдання (написання реферату та доповіді).

Теми для теоретичного вивчення:

Перший змістовий модуль:

1. Базові шифри. Частотний криптоаналіз (1 тиждень).
2. Сучасні криптографічні стандарти України (2,3 тижні).
3. Захист від SQL - ін'єкцій (4 тиждень).
4. Методи факторизації великих цілих чисел (5 тиждень).
5. Розмежування доступу в операційних системах (6, 7 тижні).

Другий змістовий модуль:

6. Малоресурсна криптографія (8, 9 тижні).
7. Антивірусне ПО (10 тиждень).
8. Методи біометричної автентифікації (11 тиждень).
9. Захист веб-застосунків(12 тиждень).
10. Розробка криптопроцесорів (13, 14 тижні).

По закінченні семестру студент повинен виконати письмовий звіт (реферат), з обраною (або іншою узгодженою з викладачем) теми та підготувати слайди і виступити з доповіддю. Індивідуальне завдання повинно бути представлено викладачеві на перевірку не пізніше 12 тижня.

Впродовж семестру передбачено проведення 2 години консультацій згідно графіку.

9. Система та критерії оцінювання курсу

Види контролю (поточний, рубіжний) проміжна атестація. Форми контролю.

Контроль передбачає проведення двох модульних контролів впродовж семестру, поточний контроль при виконанні лабораторних робіт та поточний контроль вивчення тем самостійної роботи і виконання індивідуального завдання. У підсумку проведення контрольних засобів виставляються бали на залік.

Розподіл балів:

- виконання лабораторних робіт:
- лабораторні роботи – по 5 балів за кожну,
- максимальний бал при проведенні модульного контролю:
- за першим змістовим модулем – 20 балів,
- за другим змістовим модулем – 20 балів.

зарахована індивідуальна (контрольна) робота - 25 балів.

10. Політика курсу

При організації освітнього процесу в Національному університеті «Запорізька політехніка» студенти, викладачі, методисти та адміністрація діють відповідно до наступних документів:

- Положення про організацію освітнього процесу в НУ «Запорізька політехніка» http://zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_orhanizatsiyu_osvitnoho_protseesu.pdf

- Наказ №120 від 15.04.2019 «Про планування освітнього процесу на 2019/2020 н.р.» http://zntu.edu.ua/uploads/dept_nm/Nakaz_No.120_vid_15.04.2019.pdf
- Положення про систему забезпечення НУ «Запорізька політехніка» якості освітньої діяльності та якості вищої освіти (системи внутрішнього забезпечення якості) http://zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_zabezpechennia_yakosti.pdf
- Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу НУ «Запорізька політехніка» http://zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_akademichnu_mobilnist.pdf
- Лист Міністерства освіти і науки України керівникам закладів вищої освіти від 23.10.2018 № 1/9-650 «Щодо рекомендацій з академічної доброчесності для закладів вищої освіти» <https://zakon.rada.gov.ua/rada/show/v-650729-18>

Невчасно виконані завдання, пропущені заняття відпрацьовуються в узгодженому з викладачем режимі. Пропущена лекція відпрацьовується студентом самостійно у вигляді підготовки короткого конспекту за темою заняття. Пропущена лабораторна робота виконується студентом самостійно вдома або в комп'ютерному класі, результати оцінюються викладачем.

У випадку, коли студент приймав участь у програмі академічної мобільності, можливе врахування отриманих оцінок в іншому навчальному закладі за умови відповідності навчальних планів дисциплін.