Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

IS **Кафедра інформаційної безпеки**

Безпека інформаційних систем

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки та інформаційні технології
Освітня програма	Інформаційні технології в біології та медицині
Статус дисципліни	Нормативна
Форма навчання	очна(денна)
Рік підготовки, семестр	4 курс, осінній семестр
Обсяг дисципліни	4 кредити ECTS / 120 годин (28 годин лекцій, 26 годин комп'ютерних практикумів, 66 годин СР)
Семестровий контроль/ контрольні заходи	Екзамен, модульна контрольна робота, розрахункова робота (РР)
Розклад занять	http://rozklad.kpi.ua/
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: кандидат технічних наук, Стьопочкіна Ірина Валеріївна, telegram: @ivst1113, e-mail: irst-ipt@lll.kpi.ua Лабораторні: Кіфорчук Кирило Олегович, kirill.kiforchuk@gmail.com
Розміщення курсу	Посилання на дистанційний ресурс (Платформа "Сікорський": курс Безпека інформаційних систем https://do.ipo.kpi.ua/course/view.php?id=1766 , Google classroom (лабораторний практикум) https://classroom.google.com/c/MTUzMjgyNDU2OTM5

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна "Безпека інформаційних систем" забезпечує компетентності, визначені стандартом 122 Комп'ютерні науки та інформаційні технології в частині оволодіння методиками та техніками кібербезпеки.:

Метою дисципліни є надання знань, умінь та навичок щодо методик та технік кіберзахисту із використанням сучасних криптографічних засобів, штатних засобів СКБД та ОС, механізмів захисту на рівні мережі та на рівні системних та прикладних застосунків**.**

Предметом дисципліни є засоби та заходи кібербезпеки та інформаційної безпеки.

Загальні компетентності:

ЗК 2	Здатність застосовувати знання у практичних ситуаціях

Спеціальні (фахові) компетентності:

ФК 14	Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
ФК 17	Здатність до системного аналізу та розробки медичних інформаційних систем, з урахуванням можливостей технічної реалізації, а також до аналізу характеристик таких систем з огляду на їх технічну інфраструктуру та оцінки перспектив їх подальшого розвитку.

Програмні результати навчання:

ПР 16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

В структурно-логічній схемі програми підготовки фахівця навчальна дисципліна входить до переліку нормативних дисциплін, циклу загальної підготовки.

Пререквізит. Дисципліна є нормативною, для її вивчення необхідні знання з інформаційної безпеки, та знання які студенти набувають у середній школі з інформаційних дисциплін.

Постреквізити. Отримані під час вивчення навчальної дисципліни «Безпека інформаційних систем» теоретичні знання та засвоєні практичні навички використовуються в подальшому під час вивчення навчальної дисципліни "Комп'ютерні мережі" а також є основою для підготовки дипломних робіт за спеціальністю та в подальшій практичній роботі за фахом.

3. Зміст навчальної дисципліни

Основні розділи та теми, що розглядатимуться в процесі вивчення курсу:

1. Вступ. Огляд курсу.

Розділ 1. Криптографічні методи забезпечення безпеки інформаційних систем.

Тема 1.*2.*Криптографічні методи як засіб забезпечення цілісності, конфіденційності та підтвердження автентичності інформації в інформаційній системі. Симетрична та асиметрична криптографія, сфера застосунків. Принципи побудови інфраструктури вікритого ключа. Базові алгоритми симетричної криптографії та їх застосування.

Тема 1.3. Псевдовипадкові послідовності, ентропія та інформація в задачах кібербезпеки. Моделі датчиків та генераторів ПВП. Використання ПВП у мережних та криптографічних протоколах.

Тема 1.4. Основи функціонування асиметричної криптографії, та відповідні асиметричні криптографічні алгоритми. Переваги, недоліки та використання в складі мережних протоколів.

Тема 1.5. Математичні основи алгоритму Діффі-Геллмана, його використання в мережних протоколах. Сутність, переваги та недоліки шифрування та ЕЦП RSA. Генерація сертифікатів на основі OpenSSL при клієнт-серверних взаємодіях.

Тема 1.6. Алгоритми на еліптичних кривих. Застосунки для пристроїв з суттєво обмеженими обчислювальними ресурсами.
Тема 1.7. Криптографічні протоколи для реалізації різних класів віддалених взаємодій. Протоколи віддаленого жеребкування, доведення з нульовим розголошенням. Протоколи систем електронних платежів.
Тема 1.8. Протоколи розподіленого зберігання таємниці. Протоколи віддаленого голосування.

Розділ 2. Штатні механізми безпеки інформаційної системи на рівнях ОС, СКБД
Тема 2.1. Аналіз вразливостей інформаційних систем, механізми захисту. Методики виявлення вразливостей, існуючі таксономії вразливостей та загроз. Модель порушника, модель загроз, поняття про ризики. Відповідні види механізмів захисту та запобігання реалізації загроз на основі програмних, програмно апаратних засобів.
Тема 2.2. Штатні механізми захисту ОС. Проєктування системи захисту із використанням штатних механізмів захисту ОС. Моделі управління доступом у захищених ОС.
Тема 2.3. Штатні механізми захисту на рівні СКБД. Налаштування безпеки в СКБД Oracle, My SQL. SQL – ін'єкції.

Розділ 3. Додаткові засоби захисту. Безпека інформаційної системи на рівні прикладних застосунків
Тема 3.1.Вибір додаткових засобів захисту, модель "defence-in-depth". Антивірусний захист. Проєктування захисту застосунків від несанкціонованого дослідження та модифікації. Статичний аналіз коду на слабкості, обфускація застосунків, принцип білого списку.
Тема 3.*2*. Безпека веб-застосунків. Причини вразливостей веб-застосунків та шляхи запобігання ним.

Розділ 4.Безпека інформаційної системи на рівні мережі
Тема 4.1. Вибір засобів захисту інформації в мережах. Міжмережні екрани: типи, особливості налаштування. Захист інформації при налаштуванні активного мережного обладнання (роутери, комутатори). Системи виявлення атак та вторгнень: принципи роботи, приклади. Сканери та мережні аналізатори як засоби аналізу захищеності.
Тема 4.2.Безпека мережних протоколів. Вразливості найпоширеніших протоколів стеку TCP/IP мереж. Атаки грубої сили, атаки типу «spoofing», MITM, DDoS. Безпека протоколів інтернету речей.
Тема 4.3. Безпека Wi-Fi мереж. Вразливості WEP, WPA, WPA2,3. Засоби захисту.
Тема 4.4. Виявлення аномалій та витоку даних у мережі. SIEM-системи. DLP системи. Моделі на основі машинного навчання в складі механізмів захисту.

4. Навчальні матеріали та ресурси

Потреби освітнього компонента відносно спеціального матеріально-технічного та інформаційного забезпечення: мультимедійне обладнання; доступ до мережі Internet. При дистанційному / змішаному режимі навчання використовуються сервіси Zoom/ Google meet/ Classroom.

Базова література:
1. Безпека інформаційних систем. Методичні вказівки до комп'ютерного практикуму./ Стьопочкіна І.В., Ільїн К.І. - НТУУ "КПІ ім. Ігоря Сікорського", 2020- 60 с.

2. Тарнавський Ю.А. Технології захисту інформації, 2018. Електронне мережне навчальне видання. Режим доступу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Додаткова література:

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем.- К. ВНV,2009.-608 с. Режим доступу: c.http://is.ipt.kpi.ua/wpcontent/uploads/sites/4/2015/03/Graivorovskyi_Novikov.pdf
3. Основи інформаційної безпеки: навчальний посібник/ В.А. Лужецький, А.Д. Кожуховський, О.П. Войтович.-Вінниця: ВНТУ, 2013-221 с. Режим доступу: http://voytovych.vk.vntu.edu.ua/file/329641c3933b8b8cbe161af0c43785ee.pdf
4. Shneier B. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C. Режим доступу: https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf .
5. Монографія. Архипов О.Є. Вступ до теорії ризиків: інформаційні ризики: / О.Є.Архипов. – К.: Нац. Акад. СБУ, - 2015. – 248с.
6. M. Lavreniuk, O. Novikov, 2020. Malicious and benign websites classification using machine learning methods , http://tacs.ipt.kpi.ua/article/view/209434
7. O. Kondratiuk, M. Kolomitsev, 2020. Detection and correction of database schema integrity violation based on initialization scripts. http://tacs.ipt.kpi.ua/article/view/209464
8. What is obfuscation. Режим доступу: https://www.geeksforgeeks.org/what-is-obfuscation/
9. Mobile security testing guide. Режим доступу: https://owasp.org/www-project-mobile-security-testing-guide/
10. OWASP top ten. Режим доступу: https://owasp.org/www-project-top-ten/
11. SQL injection. Режим доступу: https://owasp.org/www-community/attacks/SQL_Injection
12. Huges M. How Elliptic Curve Cryptography Works. https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/
13. Information security handbook: A Guide for Managers/ P.Bowen et al. NIST, 2006. https://www.govinfo.gov/content/pkg/GOVPUB-C13-52554e2118359961bf184fe430aa5085/pdf/GOVPUB-C13-52554e2118359961bf184fe430aa5085.pdf
14. A.Harper, S.Harris, J.Ness, C.Eagle. Gray Hat Hacking. The Ethical Hackers Handbook.- The McGraw-Hill Companies,- 2011,-721 p.
15. C. Anley, J. Heasman, F. “FX” Linder, G. Richarte The Shellcoder’s Handbook, Second Edition: Discovering and Exploiting Security Holes; Wiley Publishing, Inc., Indianapolis. -2007.-745 p.
16. C. Eagle.The IDA pro book, 2nd edition,- No Starch Press, Inc., San Francisco.- 2011.-676 p.
17. D. Stuttard, M. Pinto.The Web Application Hacker’s Handbook: Discovering and Exploiting Security Flaws.-Wiley Publishing, Inc., Indianapolis. -2008.-771 p.
18. M. H. Ligh, S. Adair, B. Hartstein, M. Richard. Malware Analyst’s CookBook.- Wiley Publishing, Inc., Canada,- 2011.-746 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для вивчення навчальної дисципліни заплановано проведення 14 лекційних та 13 комп'ютерних практикумів, під час яких студенти мають виконати модульну контрольну роботу.

Під час навчання застосовуються такі **методи навчання:**

Метод навчання	Рекомендовано при проведенні	
	Лекційних занять	Комп'ютерні практикуми
Словесний метод (лекція, бесіда, інструктаж тощо)	+	+
Наочний метод (метод ілюстрацій і метод демонстрацій)	+	+
Дискусійний метод	+	+
Частково-пошуковий або евристичний метод (організація активного пошуку рішення поставлених пізнавальних завдань)		+
Метод проблемного викладу (до викладу матеріалу ставиться проблема, формується завдання на основі різних джерел і засобів. На занятті розглядається спосіб рішення задачі).		+
Дослідницький метод (самостійна пошукова робота з літературно-інформаційних джерел / завдань тощо та проведення аналізу матеріалу / завдання).		+

5.1. Лекційні заняття

Розділ 1. Криптографічні методи забезпечення безпеки інформаційних систем

Лекція №1

Основні питання, що розглядаються на лекції

1. Вступ. Огляд курсу. РСО.
2. Криптографічні методи як засіб забезпечення цілісності, конфіденційності та підтвердження автентичності інформації в інформаційній системі. Симетрична та асиметрична криптографія, сфера застосунків. Модель побудови інфраструктури вікритого ключа. Базові алгоритми симетричної криптографії та їх застосування (на прикладі ДСТУ ГОСТ 28147:2009, AES).

[1, Розд. 3.3], [2], [4, ch.1.3,10.2, 19.1], [5, Розд.2.1-2.3, 3.1,3.2, 6.1, 6.2, 7.2]

Лекція №2

Основні питання, що розглядаються на лекції

Псевдовипадкові послідовності, ентропія та інформація в задачах кібербезпеки. Моделі датчиків та генераторів ПВП. Використання ПВП у мережних та криптографічних протоколах.

[4, ch. 8.1, 11.1,16.1,17.13], [5, Розд. 2.2, 7.2]

Лекція №3

Основні питання, що розглядаються на лекції

Основи функціонування асиметричної криптографії, та відповідні асиметричні криптографічні алгоритми. Переваги, недоліки та використання в складі мережних протоколів.

[4, 19.1], [5, 7.1-7.3]

Лекція №4

Основні питання, що розглядаються на лекції

Математичні основи алгоритму Діффі-Геллмана, його використання в мережних протоколах. Сутність, переваги та недоліки шифрування та ЕЦП RSA. Генерація сертифікатів на основі OpenSSL при клієнт-серверних взаємодіях.

[5, Розд. 7.3, 8.1, 8.4, 8.5, 8.6], [4, ch. 20.4, 22.1]

Лекція №5

Основні питання, що розглядаються на лекції

Алгоритми на еліптичних кривих. Застосунки для пристроїв з суттєво обмеженими обчислювальними ресурсами.

[4, ch.19.8], дод. літ. [9].

Лекція № 6

Основні питання, що розглядаються на лекції

Криптографічні протоколи для реалізації різних класів віддалених взаємодій. Протоколи віддаленого жеребкування, доведення з нульовим розголошенням. Протоколи систем електронних платежів.

[4, ch. 23.11, 23.12]

Лекція № 7

Основні питання, що розглядаються на лекції

Протоколи розподіленого зберігання таємниці. Протоколи віддаленого голосування.

[4, ch. 2.5, 3.6, 3.7, 23.2]

Розділ 2. Штатні механізми безпеки інформаційної системи на рівнях ОС, СКБД

Лекція №8

Основні питання, що розглядаються на лекції

Аналіз вразливостей інформаційних систем, механізми захисту. Методики виявлення вразливостей, існуючі таксономії вразливостей та загроз. Модель порушника, модель загроз на основі методики STRIDE, поняття про ризики. Відповідні види механізмів захисту та запобігання реалізації загроз на основі програмних, програмно апаратних засобів.

[1,Розд. 2, 5], [2], [3, 2.3, 2.7] Дод.літ.[1], [2]. [5], [10, ch.10.1]

Питання на СРС: Керування ризиками, оцінка ризиків. Дод.літ. [10, ch.10.2, 10.3]

Лекція № 9

Основні питання, що розглядаються на лекції

1. Штатні механізми захисту ОС. Проєктування системи захисту із використанням штатних механізмів захисту ОС. Моделі управління доступом у захищених ОС.

[1, Розд. 11,12,13], [2].

Питання на СРС: Вибір сервісів інформаційної безпеки, дод. літ.[10, ch.12.2, 12.3]

2. Штатні механізми захисту на рівні СКБД. Налаштування безпеки в СКБД Oracle, My SQL. SQL – ін’єкції.

[2], дод. літ. [4],[8], [3, Розд.1.5.4, 2.2.5].

Розділ 3. Додаткові засоби захисту. Безпека інформаційної системи на рівні прикладних застосунків

Лекція №10

Основні питання, що розглядаються на лекції

Вибір додаткових засобів захисту, модель “defence-in-depth”. Антивірусний захист. Проєктування захисту застосунків від несанкціонованого дослідження та модифікації. Статичний аналіз коду на слабкості, обфускація застосунків, принцип білого списку.
[1, Розд. 6], [2], [3, 2.4] Дод. літ. [12],[13]
Питання на СРС: 1.Чеклісти безпеки програмного забезпечення, дод. літ. [10, ch.12.4]

Лекція № 11

Основні питання, що розглядаються на лекції

1. Основні принципи дії сучасних руткитів (метод DKOM, перехоплення функцій API в режимі користувача (раннє, пізнє звязування), модифікація машинного коду програми, модифікація таблиці імпорту, перехоплення функцій LoadLibrary та GetProcAddress , модифікація DLL, модифікація програмного коду API), перехоплення функцій ядра), - ознайомитись. Дод. літ.[12],[15]
2. Безпека веб-застосунків. Причини вразливостей веб-застосунків та шляхи запобігання ним.

[1,Розд. 8.3.2, 17.2], Дод.літ. [3],[7], [14]

Розділ 4.Безпека інформаційної системи на рівні мережі

Лекція №12

Основні питання, що розглядаються на лекції

Вибір засобів захисту інформації в мережах. Міжмережні екрани: типи, особливості налаштування. Захист інформації при налаштуванні активного мережного обладнання (роутери, комутатори). Системи виявлення атак та вторгнень: принципи роботи, приклади. Сканери та мережні аналізатори як засоби аналізу захищеності.
[1, Розд. 15, 18.3, 18.4], [3, Розд. 6.3, 6.4]

Лекція №13

Основні питання, що розглядаються на лекції

Безпека мережних протоколів. Вразливості найпоширеніших протоколів
стеку TCP/IP мереж. Атаки грубої сили, атаки типу «spoofing», MITM, DDoS. Безпека протоколів інтернету речей.
[1, Розд.15, 16]
Питання на СРС: тестування на проникнення із використанням Metasploit [1, Розд.6.6.3]

Лекція № 14

Основні питання, що розглядаються на лекції

1. Безпека Wi-Fi мереж. Вразливості WEP, WPA, WPA2,3. Засоби захисту.
   [1, Розд. 15], стандарти IEEE 802.11, 802.11i, Wi-Fi Alliance WPA3 Security Considerations, https://www.wi-fi.org/file/wpa3-security-considerations
2. Виявлення аномалій та витоку даних у мережі. SIEM-системи. DLP системи. Моделі на основі машинного навчання в складі механізмів захисту.
   [1, 18.3.4, 18.3.5] Дод. літ.[10, ch.13]
   Питання на СРС: Виявлення та аналіз інцидентів безпеки, дод. літ. [10, ch.13.2]

5.2. Комп'ютерні практикуми

Теми комп’ютерних практикумів (зміст робіт наведено у [2])

№ КП	Зміст комп’ютерного практикуму	Кількість ауд. годин
1.	Запровадження парольної автентифікації та розмежування доступу у програмний застосунок	4
2.	Захист застосунків від несанкціонованого використання і копіювання	4
3.	Використання криптографічних функцій для захисту інформації	4
4.	Аналіз механізмів захисту застосунку та застосування обфускації	4
5.	Автоматизований пошук вразливостей у вихідних текстах програмного забезпечення, що написані на мові високого рівня.	4
6	Механізми захисту операційних систем	4
	Модульна контрольна робота	2
	Всього	26 годин

6. Самостійна робота студента

Відповідно до наказу НОН/39/2023 від 10.02.2023 "Про планування та організацію освітнього процесу", орієнтовні середні норми часу для СРС наступні:

- підготовка до аудиторних занять – 30 год.

- підготовка до МКР - 2 год.

- підготовка до екзамену - 24 год.

- виконання РР – 10 год.

.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Відвідування занять не оцінюється, але рекомендується. Контроль відвідування проводиться викладачем вибірково.

Комп’ютерні практикуми захищаються у відповідності до встановлених дедлайнів на протязі семестру. При невчасному захисті комп’ютерного практикуму бали знімаються до мінімального (відповідає рівню “задовільно”).

Під час захисту практикумів а також під час контрольних заходів студентами повинна дотримуватись політика академічної доброчесності, згідно Кодексу Честі НТУУ “КПІ”.

Пропущені контрольні заходи

Результат модульної контрольної роботи для студента(-ки), який не з’явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.

Штрафні та заохочувальні бали

Заохочувальні бали		Штрафні бали	
Критерій	Ваговий бал	Критерій	Ваговий бал
Присутність та активність на більшості занять (для очного навчання)	+5 балів	Невчасне подання звіту з комп'ютерного практикуму. Дедлайни узгоджуються зі студентами	-2 бали

Однак, згідно положенняhttps://osvita.kpi.ua/node/37 п.2.7, сума заохочувальних або штрафних балів не може перевищувати 10% рейтингової шкали.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". Детальніше: https://kpi.ua/code.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". Детальніше: https://kpi.ua/code.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студент має право оскаржити результати контрольного заходу згідно затвердженого положення Про апеляції в КПІ імені Ігоря Сікорського (затверджено наказом №НОН/128/2021 від 20.05.2021 р.) - https://osvita.kpi.ua/index.php/node/182

Інклюзивне навчання

Навчальна дисципліна "Теорія вибору альтернатив" може викладатися для більшості студентів з особливими освітніми потребами, окрім студентів з серйозними вадами зору, які не дозволяють виконувати завдання за допомогою персональних комп'ютерів, ноутбуків та/або інших технічних засобів.

Дистанційне навчання

Дистанційне навчання відбувається через Платформу дистанційного навчання "Сікорський""Google клас".

Дистанційне навчання через проходження додаткових он-лайн курсів за певною тематикою не допускається.

Список курсів пропонується викладачем після виявлення бажання студентами (оскільки банк доступних курсів поновлюється майже щомісяця).

Виконання контрольних заходів може здійснюється під час самостійної роботи студентів у дистанційному режимі (з можливістю консультування з викладачем через електронну пошту, соціальні мережі).

Навчання іноземною мовою

Навчання англійською мовою здійснюється лише для студентів-іноземців.

За бажанням студентів, допускається вивчення матеріалу за допомогою англомовних онлайн-курсів за тематикою, яка відповідає тематиці конкретних занять.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: здійснюється під час навчальних занять і має на меті перевірити рівень підготовки студентів до навчальних занять. Під час комп'ютерних практикумів проводиться виконання та захист 6 комп'ютерних звітів. Модульна контрольна робота проводиться в кінці семестру, після закінчення викладання теоретичного матеріалу. Виконання та захист індивідуального завдання (РР).

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Є два можливих результати календарного контролю: атестований (а) та неатестований (н/а). Результат залежить від кількості набраних балів на момент проведення календарного контролю відповідно до вимог КПІ ім. Ігоря Сікорського.

Критерій			Перша атестація	Друга атестація
Термін атестації			8-ий тиждень	14-ий тиждень
Умови отримання атестації	Поточний рейтинг		≥ 9 балів	≥ 12 балів
	Поточний контрольний захід	Модульна контрольна робота	–	-
	Комп'ютерні практикуми	КП №1	+	+
		КП №2	+	+
		КП №3	+	+
		КП №4	–	+
		КП №5	–	–
		КП №6	–	–

***Семестровий контроль**:* екзамен.

Система оцінювання (поточний контроль):

№ з/п	Контрольний захід	%	Макс. бал	Ваговий коеф.	Кіл-ть	Всього
1.	МКР	15	5	3	1	15
2.	Розрахункова робота	15	5	3	1	15
3.	Комп'ютерні практикуми	30	5	1	6	30
4	Екзамен	40	5	8	1	40
	Всього					100

Модульна контрольна робота
Ваговий бал - 5. Кількість завдань в МКР - 3. Максимальна кількість балів за МКР = 5 балів * 3 завдання =15 балів
Критерій оцінювання МКР:

«Відмінно», відповідь правильна (не менше 90% потрібної інформації)	5 балів
«Добре», є несуттєві помилки у відповіді (не менше 75% потрібної інформації)	4 бали
«Достатньо», є недоліки у відповіді та певні помилки (не менше 60% потрібної інформації).	3 бали
«Незадовільно»,відповідь відсутня або не відповідає вимогам до «Достатньо»	0 балів

Розрахункова робота
Ваговий бал - 5. Оцінювання РР проводиться за 3 компонентами: розрахунок, оформлення та захист РР. Максимальна кількість балів за РР = 5 балів * 3 компоненти =15 балів
Критерій оцінювання компоненту РР:

«Відмінно» -не менше 90% потрібної інформації при розрахунках та захисті РР, а також дотримання вимог до оформлення звіту з РР.	5 балів
«Добре» -не менше 75% потрібної інформації при розрахунках та захисті РР, а також є несуттєві недоліки при оформленні звіту з РР.	4 бали
«Достатньо»- не менше 60% потрібної інформації при розрахунках та захисті РР, а також є суттєві недоліки при оформленні звіту з РР.	3 бали
«Незадовільно»,відповідь відсутня або не відповідає вимогам до «Достатньо»	0 балів

Звіт з комп'ютерного практикуму
Ваговий бал - 5. Максимальна кількість балів за звіти = 5 балів * 6 звітів = 30 балів
Критерій оцінювання звіту з КП:

«Відмінно» -не менше 90% потрібної інформації при розрахунках та захисті КП.	5 балів
«Добре» -не менше 75% потрібної інформації при розрахунках та захисті КП.	4 бали
«Достатньо»- не менше 60% потрібної інформації при розрахунках та захисті КП	3 бали
«Незадовільно»,відповідь відсутня або не відповідає вимогам до «Достатньо»	0 балів

Здобувач допускається до іспиту за результатами роботи в семестрі, якщо має підсумковий рейтинг за семестр не менше 30 балів та виконав умови допуску до семестрового контролю, які визначені РСО: виконання модульної контрольної роботи, виконання та захист всіх звітів, виконання та захист РР..

Екзаменаційна робота
Кількість запитань у кожному екзаменаційному білеті – 8.
Ваговий бал запитання – 5.
Максимальна кількість балів за всі питання екзаменаційного білета = 8 запитань * 5 балів = 40 балів

«Відмінно», відповідь правильна (не менше 90% потрібної інформації)	5 балів
«Добре», є несуттєві помилки у відповіді (не менше 75% потрібної інформації)	4 бали

«Достатньо», є недоліки у відповіді та певні помилки (не менше 60% потрібної інформації).	3 бали
«Незадовільно»,відповідь відсутня або не відповідає вимогам до «Достатньо»	0 балів

Необов'язкові умови допуску до іспиту:

1. Активність на комп'ютерних практикумах.
2. Позитивний результат першої атестації та другої атестації.
3. Відвідування лекційних занять.

Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Кількість балів	Оцінка за університетською шкалою
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

- *Перелік запитань наведено в Електронному кампусі КПІ ім. Ігоря Сікорського та в папці курсу на платформі «Сікорський».*
- *Сертифікати проходження дистанційних чи онлайн курсів за відповідною тематикою можуть бути зараховані за умови виконання вимог, наведених у Наказі №НОН/157/2023 від 09.05.2023р. «Про затвердження положення про визнання в КПІ ім. Ігоря Сікорського результатів навчання, набутих у неформальній/інформальній освіті». https://osvita.kpi.ua/node/179*

Робочу програму навчальної дисципліни (силабус):
Склав: доц. каф. Інформаційної безпеки Стьопочкіна Ірина Валеріївна
Ухвалено кафедрою інформаційної безпеки (протокол №5/2023 від 22.06.2023)
Погоджено Методичною комісією факультету біомедичної інженерії (протокол №1 від 01.09.2023)