Чернівецький національний університет імені Юрія Федьковича

(повне найменування закладу вищої освіти)

Навчально-науковий інститут фізико-технічних і комп'ютерних наук

(назва інституту/факультету)

Кафедра комп'ютерних систем та мереж

(назва кафедри)

СИЛАБУС

навчальної дисципліни

Кібербезпека високопродуктивних комп'ютерних систем

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

вибіркова

(обов'язкова чи вибіркова)

Освітньо-професійна програма–*"Комп'ютерна інженерія","Програмування мобільних і вбудованих комп'ютерних систем та засобів Інтернету речей"*

Спеціальність *123 – Комп'ютерна інженерія*

(шифр і назва спеціальності)

Галузь знань *12 – Інформаційні технології*

(шифр і назва галузі знань)

Рівень вищої освіти – *перший (бакалаврський)*

(вказати: перший (бакалаврський)/другий (магістерський)/третій (освітньо-науковий))

Навчально-науковий інститут фізико-технічних і комп'ютерних наук

(назва факультету / інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання – *українська*

(мова, на якій читається дисципліна)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ, кандидат техн. наук,

(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Кількість кредитів: 4

Форми навчальної діяльності: лекції, лабораторні роботи, самостійна робота

Форма підсумкового контролю: іспит

Профайл викладача (-ів) https://csn.chnu.edu.ua, https://csn.chnu.edu.ua/employees/ivanushhak-nataliya-myhajlivna/

Контактний тел. +(38) 0372 50 94 32 (кафедра КСМ) – Іванущак Н.М.

E-mail: n.ivanuschak@chnu.edu.ua

Сторінка курсу в Moodle https://moodle.chnu.edu.ua/course/view.php?id=1355

Консультації *on-line: середа з 17.00 до 18.00*

1. Анотація дисципліни

Курс «Кібербезпека високопродуктивних комп'ютерних систем» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань з основних положень кібербезпеки, знайомить з найбільш розповсюдженими типами шифрів та методами криптоаналізу, криптографічними протоколами (електронні гроші, електронний підпис, електронне голосування тощо). Пояснюється математична теорія, яка лежить в основі кібербезпеки (а саме основні поняття сучасної теорії чисел). Перевагою даного курсу є поглиблення професійних знань у межах обраної професійної кваліфікації, здобуття додаткових загальних і загально-професійних компетентностей у сфері технологій захисту інформації. Введення курсу в навчальний план дозволяє надати студентам додаткові знання та практичні навички, які вони зможуть застосовувати як при подальшому навчанні, так і в майбутній професійній діяльності.

2. Мета навчальної дисципліни: ознайомлення з теоретичними основами кібербезпеки, придбання навичок в практичному використанні, постановці і розв'язанні задач шифрування інформації, розуміння суті інформаційних процесів в криптографічних системах, робота криптографічних протоколів у високопродуктивних комп'ютерних системах.

Завдання випливають з ролі дисципліни у системі підготовки спеціалістів: вивчення студентами основних теоретичних понять з кібербезпеки; уміння застосовувати їх для розв'язку завдань, що ставить перед ними виробництво; набуття студентами практичних навичок криптографії та криптоаналізу; вільне володіння основними алгоритмами криптографії; розуміння основних понять і сучасного стану даного предмету.

3. Пререквізити. Для коректного розуміння і засвоєння матеріалу даного курсу слухачі повинні попередньо пройти курси: Комп'ютерна електроніка, Теорія електричних кіл, Комп'ютерна логіка, Основи алгоритмізації та програмування. Результати навчання за цим курсом потрібні при вивченні дисципліни Захист інформації в комп'ютерних системах, Технологія IoT Blockchain, Кібербезпека Cisco та виконанні дипломного проекту.

4. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

4.1. Знати: найновіші досягнення кібербезпеки високопродуктивних комп'ютерних систем; характеристики основних найбільш відомих криптографічних алгоритмів; основні алгоритми електронного цифрового підпису; методи управління криптографічними ключами; організаційно-правові аспекти криптографічного захисту в Україні.

4.2. Вміти: застосовувати криптографічні алгоритми для визначеного програмою класу задач; розробляти програмне забезпечення з елементами криптографічного захисту конфіденційності інформації; розробляти програмні продукти з можливістю криптографічного захисту цілісності інформації; реалізовувати алгоритми розподілу криптографічних ключів; розробляти програмні продукти з використанням криптографічного інтерфейсу Microsoft CryptoAPI.

4.3. Набути компетентностей:

ЗК – загальних

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК2. Здатність вчитися і оволодівати сучасними знаннями.
ЗК3. Здатність застосовувати знання у практичних ситуаціях.
ЗК7. Вміння виявляти, ставити та вирішувати проблеми.
ЗК8. Здатність працювати в команді.

ФК – спеціальних (фахових)

ФК2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

ФК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

ФК6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

ФК8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

ФК9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

ПРН - програмні результати навчання

ПРН3. Знати новітні технології в галузі комп'ютерної інженерії.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

ПРН9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН16*. Вміти оцінювати результати обробки даних в інформаційно-вимірювальних системах і проводити пошук оптимальних рішень для їх покращення на основі застосування технології дискретної обробки інформаційних сигналів у комп'ютерній інженерії.

ПРН18. Використовувати інформаційні технології та для ефективного спілкування на професійному та соціальному рівнях.

ПРН19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

ПРН20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

5. Опис навчальної дисципліни
5.1. Загальна інформація

Назва навчальної дисципліни *Кібербезпека високопродуктивних КС*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсум-кового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	**4**	**7**	**4**	**120**	**2**	**30**	**15**	**-**	**15**	**60**	**-**	**Іспит**
Заочна	**4**	**7**	**4**	**120**	**2**	**8**	**4**	**-**	**4**	**104**	**-**	**Іспит**

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 1,0 ((30+30)/60);
для заочної форми навчання – 0,15 ((8+8)/104).

5.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Математична теорія кібербезпеки												
Тема 1. Основні етапи розвитку кібербезпеки.	14	4	2	2	-	6	13	1	0	0	-	12
Тема 2. Основи теорії чисел.	16	2	3	3	-	8	15	1	1	1	-	12
Тема 3. Потокові та блокові шифри.	16	6	1	1	-	8	15	1	1	1	-	12
Тема 4. Симетричні та асиметричні криптосистеми.	14	4	1	1	-	8	17	1	0	0	-	16
Разом за змістовим модулем 1	60	16	7	7	-	30	60	4	2	2	-	52
Змістовий модуль 2. Основи кібербезпеки високопродуктивних систем												
Тема 5. Криптографічні протоколи електронного цифрового підпису.	18	4	3	3	-	8	18	1	0	1	-	16
Тема 6. Захист інформації на мережевому рівні. Криптографічні протоколи комп'ютерних мереж.	26	6	4	4	-	12	20	2	1	1	-	16
Тема 7. Математичні основи генерування псевдовипадкових послідовностей.	16	4	1	1	-	10	22	1	1	0	-	20
Разом за змістовим модулем 2	60	14	8	8	-	30	60	4	2	2	-	52
Усього годин	120	30	15	15	-	60	120	8	4	4	-	104

5.3. Тематика лабораторних занять

№	Назва теми
1.	Шифрувальна система на основі шифру простої заміни.
2.	Шифрувальна система на основі афінної системи Цезаря.
3.	Шифрувальна система на основі шифру гамування.
4.	Система блочного шифрування S-DES.
5.	Використання шифрувальної системи RSA для цифрового підпису.
6.	Відкритий розподіл криптографічних ключів за алгоритмом Діффі-Хелмана.
7.	Потоковий шифр на основі генератора BBS.

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет- ресурсах: https://moodle.chnu.edu.ua/course/view.php?id=1355

5.4. Самостійна робота

№ з/п	Назва теми
1	Математичні основи теорії захисту інформації.
2	Порівняльний аналіз криптографічних методів аутентифікації.
3	Використання полів Галуа в кібербезпеці.
4	Кібербезпека на мережному рівні. Протокол IPSec (IP Security).
5	Кібербезпека на мережному рівні. Віртуальні приватні мережі.
6	Кібербезпека на мережному рівні. Протокол SSH (Secure Shell).
7	Кібербезпека на мережному рівні. Протокол PGP (Pretty Good Privasy).
8	Порівняльний аналіз криптосистеми Blowfish.
9	Порівняльний аналіз криптосистеми Serpent.
10	Протоколи «з нульовим розголошенням».

6. Форми і методи навчання

Форми навчання – це проблемні й оглядові лекції, лабораторні заняття, заняття із застосуванням комп'ютерної та телекомунікаційної техніки, інтерактивні заняття з навчанням одних студентів іншими, інтегровані заняття, проблемні заняття, відеолекції, відеозаняття і відеоконференції засобами Google Meet, Zoom, заняття з використанням системи електронного навчання Moodle.

Методи: проблемний виклад матеріалу, частково-пошукові та дослідницькі лабораторні практикуми, презентації, консультації і дискусії, робота в інтернет-класі: електронні лекції, лабораторні роботи, дистанційні консультації та ін., спрямовані на активізацію і стимулювання навчально-пізнавальної діяльності студентів.

Підходи до навчання: використовуються студентоцентрований, проблемно-орієнтований, діяльнісний, комунікативний, професійно-орієнований, міждисциплінарний підходи.

Для викладання матеріалів з навчальної дисципліни «Кібербезпека високопродуктивних комп’ютерних систем» використовуються такі методи навчання.

6.1. Словесні методи навчання. Навчальна лекція

За допомогою даного методу забезпечується усне викладення матеріалу великими ємністю й складністю логічних побудов, доказів і узагальнень. В ході лекції використовуються прийоми усного викладення інформації, підтримання уваги протягом тривалого часу, активізації мислення студентів, прийоми забезпечення логічного запам’ятовування, переконання, аргументації, доказів, класифікації, систематизації і узагальнення. В залежності від специфіки лекційного матеріалу іноді використовується лекція-діалог.

6.2. Індуктивний метод навчання

Даний метод навчання використовується в рамках лекційних занять, коли матеріал носить, здебільшого, фактичний характер. В рамках лабораторних занять метод застосовується при виконанні технічних задач, коли студенти використовують раніше здобуті теоретичні знання при роботі з конкретними пристроями (комп’ютерами) та програмними продуктами.

6.3. Репродуктивний метод навчання

Даний метод навчання використовується в рамках лекційних і лабораторних занять, а також під час самостійної роботи студентів. Метод передбачає роботу студентів за визначеним алгоритмом. Згідно з методом для виконання завдань студентам надаються методичні вказівки, правила і навчальні приклади.

6.4. Проблемно-пошукові методи навчання

Проблемно-пошукові методи застосовуються в ході проблемного навчання, а саме в процесі виконання лабораторних робіт та індивідуальних науково-дослідних завдань, де під проблемною ситуацією треба вважати невідповідність між тим, що вивчається і вже вивченим. При використанні проблемно-пошукових методів навчання викладач використовує такі прийоми: створює проблемну ситуацію (ставить питання, пропонує задачу, експериментальне завдання), організує колективне обговорення можливих підходів до рішення проблемної ситуації, стимулює висування гіпотез, тощо. Студенти роблять припущення про шляхи вирішення проблемної ситуації, узагальнюють раніше набуті знання, виявляють причини явищ, пояснюють їхнє походження, вибирають найбільш раціональний варіант вирішення проблемної ситуації. Викладач обов'язково керує цим процесом на всіх етапах, а також за допомогою запитань-підказок. Також даний метод використовується при опрацюванні матеріалів в системі дистанційної освіти «Moodle».

6.5. Наочний метод навчання

Наочний метод достатньо важливий для студентів, оскільки забезпечує візуальне подання навчального матеріалу, зокрема, з використанням інформаційно-комунікаційних технологій. При викладанні дисципліни наочний метод навчання поєднується зі словесними методами для представлення інформації у вигляді таблиць, рисунків, схем та діаграм.

7. Система контролю та оцінювання

Засобами оцінювання та демонстрування результатів навчання є

- контрольні роботи;
- стандартизовані тести;
- презентації результатів виконаних завдань та досліджень;
- завдання на лабораторному обладнанні.

Формами поточного контролю рівня знань є усна та письмова відповідь студента при захисті виконаних лабораторних робіт, кількість отриманих балів при виконанні тестового завдання, а також письмова відповідь при написанні модульних контрольних робіт. Формами підсумкового контролю рівня знань є усна та письмова відповідь студента при здачі іспиту.

7.1. Критерії оцінювання результатів навчання з навчальної дисципліни

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

У залежності від характеру відповіді студента кількість балів за кожний вид діяльності може бути визначена за наступними критеріями:

К-ть балів	Критерії оцінки
Max	Студент дає вичерпну відповідь на поставлене запитання
0,8 · Max	Студент при відповіді на поставлене запитання припустився незначних неточностей, які не впливають на суть відповіді
0,6 · Max	Студент при відповіді на поставлене запитання припустився помилок, які виправляє за допомогою викладача; в середньому може дати правильні відповіді на 50% питань теми
0,4 · Max	Студент при відповіді на поставлене запитання припустився суттєвих помилок, які все ж таки виправляє за допомогою викладача; дає правильні відповіді на 30% питань теми
0,2 · Max	Студент за допомогою викладача фрагментарно відповідає на запитання, проте не в повній мірі володіє мінімальним рівнем знань з даного питання
0	Характер відповідей дає підставу стверджувати, що студент неправильно зрозумів суть питання чи не знав правильної відповіді, а тому відповідав, припускаючись грубих помилок.

Примітка: за Max прийнято максимальну оцінку для даного виду діяльності; заокруглення проводиться до одиниць балу.

Шкала та критерії оцінювання: національна та ЄКТС (Європейська кредитна трансферно-накопичувальна система, ECTS)

Оцінка за шкалою ЄКТС	Пояснення	Оцінка за 100-бальною шкалою	Оцінка за національною шкалою
A	відмінно	**90 – 100**	**відмінно**
B	дуже добре	**80-89**	**добре**
C	добре	**70-79**	
D	задовільно	**60-69**	**задовільно**
E	достатньо	**50-59**	
FX	(незадовільно) з можливістю повторного складання	**35-49**	**незадовільно**
F	(незадовільно) з обов'язковим повторним курсом	**1-34**	

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Підсумковий тест (іспит)	Сума балів
Змістовий модуль 1					Змістовий модуль 2				40	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
5	5	5	5	10	5	5	10	10		

7.2. Перелік тем і розподіл максимально можливої кількості балів, які отримують студенти за виконання всіх видів навчальної діяльності

Змістовий модуль 1. Математична теорія кібербезпеки

Т1. Основні етапи розвитку кібербезпеки (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т2. Основи теорії чисел (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т3. Потокові та блокові шифри (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т4. Симетричні та асиметричні криптосистеми (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

М1 – модульна контрольна робота №1 (10 балів)

Змістовий модуль 2. Основи кібербезпеки високопродуктивних систем

Т5. Криптографічні протоколи електронного цифрового підпису (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т6. Захист інформації на мережевому рівні. Криптографічні протоколи комп’ютерних мереж. (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та матеріалів практичних занять – 5 балів).

Т7. Математичні основи генерування псевдовипадкових послідовностей (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та матеріалів практичних занять – 10 балів).

М2 – модульна контрольна робота №2 (10 балів).

Підсумковий контроль (**іспит**) – 40 балів: підсумкове тестування студентів у системі Moodle. **Сумарна кількість балів** – 100.

7.3. Умови зарахування результатів неформальної освіти

Студент, згідно Положення ЧНУ «Про неформальну освіту» може отримати додаткові бали, або бути звільненим від окремих видів роботи з окремих тем, якщо у нього наявні сертифікати про неформальну освіту з проблем, які вивчаються на дисципліні «Кібербезпека високопродуктивних систем».

Також, як виконані види роботи з відповідних тем зараховуються студенту бали за наукові публікації у матеріалах науково-практичних конференцій та фахових чи апробаційних виданнях.

7.4. Політика курсу

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).

Академічна доброчесність: посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Відвідування: Відвідування занять є обов’язковим. Засвоєння пропущеної теми лекції з поважної причини перевіряється під час складання підсумкового контролю. Пропуск лекції з неповажної причини відпрацьовується студентом (співбесіда, реферат тощо). Пропущені практичні та лабораторні заняття, незалежно від причини пропуску, студент відпрацьовує згідно з графіком консультацій.

8. Рекомендована література

Фахова (основна)

1. Остапов С.Е.,Валь Л.О. Основи криптографії. Чернівці: Книги-ХХІ, 2008. – 188 с.
2. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 стор.
3. Buchmann J. A., Introduction to cryptography, second edition, 2004, Springer Verlag, New York.
4. Koshy T., Elementary Number Theory with Applications, 2007, 2nd edition, Elsevier, Amsterdam.

Допоміжна

1. Coutinho S., The Mathematics of Ciphers. Number Theory and RSA Criptography, 1999, A. K. Peters, Natick, Massachusetts.
2. Rosen K. H., Elementary Number Theory, 2011, 6th edition, Addison Wesley, Boston MA.

3. W. Stein, Elementary Number Theory: Primes, Congruences, and Secrets. A computational Approach, 2009, Springer-Verlag, New York.
4. Young A. L., Mathematical Ciphers: from Caesar to RSA, 2006, American Mathematical Society, Providence, RA.

9. Інформаційні ресурси

1. https://csn.chnu.edu.ua/about-us/ok-rivni/
2. https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-programuvannya-mobilnyh-i-vbudovanyh-komp-yuternyh-system-ta-zasobiv-internetu-rechej-bakalavrat-4-r/
3. https://moodle.chnu.edu.ua/course/view.php?id=1355