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

ОК29. Захист інформації в комп'ютерних системах

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

обов'язкова

(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: залік

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=1357

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

1. Анотація дисципліни

Курс Захист інформації в комп’ютерних системах призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань з теорії захисту інформації, вміння формування основних загроз та ризиків організації та персоналу в кіберпросторі, розуміння мінімальних вимог та обмежень під час роботи в сфері кібербезпеки.

2. Мета навчальної дисципліни: надання студентам систематизованих знань з основ захисту інформації: мети, завдань, принципів організації комплексних систем захисту інформації на основі нормативних документів; забезпечення вмінням боротьби з загрозами інформації в комп’ютерних мережах; теоретичними і практичними знаннями засобів захисту інформації від витоку технічними каналами; методами боротьби з несанкціонованим доступом до інформації з обмеженим доступом; використанням програмно-апаратних методів для побудови систем захисту.

Завдання навчальної дисципліни Захист інформації в комп’ютерних системах - вивчення студентами основних теоретичних понять з захисту інформації; уміння застосовувати їх для розв’язку завдань, що ставить перед ними виробництво; набуття студентами практичних навичок; вільне володіння основними методами захисту інформації; 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 логіка, Архітектура комп’ютерів, Комп’ютерні мережі, Організації баз даних. Результати навчання за цим курсом потрібні при вивченні дисципліни Комп’ютерний захист фінансової інформації, Технологія IoT Blockchain, Кібербезпека Cisco та виконанні дипломного проекту.

4. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

4.1. Знати: найновіші досягнення в галузі захисту інформації; характеристики основних підсистем ідентифікації та аутентифікації; характеристики основних механізмів доступу; характеристики підсистем захисту основних класів операційних систем; основні принципи формування політики безпеки підприємства; основні канали витоку інформації та методи боротьби з ним; критерії захищеності автоматизованих систем; характеристики основних стандартних профілів захищеності автоматизованих систем; основні характеристики захищених протоколів передавання даних.

4.2. Вміти: будувати політику безпеки в комп’ютерних мережах на основі аналізу загроз та оцінки ризиків; використовувати програмні, організаційно-адміністративні та технічні засоби захисту інформації; орієнтуватися в законодавчо-нормативній базі в галузі захисту інформації; правильно налагоджувати підсистеми захисту сучасних операційних систем; правильно визначати та застосовувати критерії захищеності автоматизованих систем.

4.3. Набути компетентностей:

ЗК – загальних

ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК7. Вміння виявляти, ставити та вирішувати проблеми.

ЗК8. Здатність працювати в команді.

ФК – фахових (спеціальних)

ФК5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

ФК7. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного 8 устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

ФК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

ФК15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

ФК16. Здатність застосовувати технології комп'ютерних систем і мереж, дискретної обробки інформації та числових методів для реалізації інформаційно-вимірювальних систем і систем передачі даних.

ПРН – програмних результатів навчання

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

ПРН8. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

5. Опис навчальної дисципліни

5.1. Загальна інформація

Назва навчальної дисципліни *ОК29 Захист інформації в комп'ютерних системах*													
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**	**24**	**-**	**-**	**24**	**72**	**-**	**Залік**
Заочна	**4**	**7**	**4**	**120**	**2**	**6**	**-**	**-**	**6**	**108**	**-**	**Залік**

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 0,66 ((24+24)/72);
для заочної форми навчання – 0,11 ((6+6)/108).

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. Політика безпеки підприємства												
Тема 1. Основні поняття та визначення захисту інформації.	15	3	-	3	-	9	15	1	-	1	-	13
Тема 2. Формальний та неформальний підхід опису загроз комп'ютерної системи.	15	3	-	3	-	9	15	0	-	1	-	13
Тема 3. Шкідливі програми та кіберзлочини. Політика безпеки.	15	3	-	3	-	9	15	1	-	0	-	14
Тема 4. Стандартизовані критерії оцінки захищеності інформації від НСД.	15	3	-	3	-	9	15	1	-	1	-	14
Разом за змістовим модулем 1	60	12	-	12	-	36	60	3	-	3	-	54
Змістовий модуль 2. Захист інформації в сучасних операційних системах												
Тема 5. Контроль цілісності даних і аутентифікація повідомлень.	15	3	-	3	-	9	15	1	-	1	-	13
Тема 6. Протоколи аутентифікації.	15	3	-	3	-	9	15	0	-	1	-	13
Тема 7. Механізми та протоколи керування криптографічними ключами.	15	3	-	3	-	9	15	1	-	1	-	14
Тема 8. Стеганографія. Основні принципи захисту інформації при підключенні до мережі Інтернет.	15	3	-	3	-	9	15	1		0		14
Разом за змістовим модулем 2	60	12	-	12	-	36	60	3	-	3	-	54
Усього годин	**120**	**24**	**-**	**24**	**-**	**72**	**120**	**6**	**-**	**6**	**-**	**108**

5.3. Теми лабораторних занять

№	Назва теми
1.	Механізми захисту операційної системи Windows (керування обліковими записами).
2.	Захист реєстру операційної системи Windows
3.	Модель безпеки операційної системи Windows
4.	Налаштування політики безпеки операційної системи Windows
5.	Вивчення можливостей захисту шифрованої файлової системи (EFS) Windows
6.	Дослідження можливостей брандмауера Windows
7.	Реалізація дискреційної моделі політики безпеки
8.	Реалізація мандатної моделі політики безпеки

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет- ресурсі: https://moodle.chnu.edu.ua/course/view.php?id=1357

Програмне забезпечення для виконання лабораторних робіт: операційна система Windows із адміністративними правами.

5.4. Самостійна робота

№ з/п	Назва теми
1	Огляд підсистеми захисту операційної системи Linux Tails
2	Огляд підсистеми захисту операційної системи OpenBSD
3	Криптографічні засоби захисту операційної системи Linux Ubuntu
4	Огляд властивостей підсистеми захисту AppArmor
5	Засоби захисту операційної системи Android
6	Засоби захисту операційної системи iOS
7	Аутентифікація користувачів на основі токенів безпеки
8	Моделювання підсистеми керування доступом та аудиту

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 «Захист інформації в комп’ютерних системах» 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 національною шкалою (залік)	Оцінка за шкалою ЄКТС	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Зараховано	**A (90-100)**	Зараховано
	B (80-89)	
	C (70-79)	
	D (60-69)	
	E (50-59)	
Не зараховано	**FX (35-49)**	Не зараховано з можливістю повторного складання
	F (1-34)	Не зараховано з обов'язковим повторним вивченням дисципліни

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота										**Підсумковий контроль (залік)**	**Сума балів**
Змістовий модуль 1					**Змістовий модуль 2**					40	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	Т8	М2		
5	5	5	5	10	5	5	5	5	10		

Т1 ... Т8 – теми змістових модулів; М1, М2 – модульні контрольні роботи

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

Змістовий модуль 1. Політика безпеки підприємства

Т1. Основні поняття та визначення захисту інформації (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т2. Формальний та неформальний підхід опису загроз комп'ютерної системи (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т3. Шкідливі програми та кіберзлочини. Політика безпеки (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т4. Стандартизовані критерії оцінки захищеності інформації від НСД (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

М1 – модульна контрольна робота №1 (10 балів).

Змістовий модуль 2. Захист інформації в сучасних операційних системах

Т5. Контроль цілісності даних і аутентифікація повідомлень (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т6. Протоколи аутентифікації (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т7. Механізми та протоколи керування криптографічними ключами (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

Т8. Стеганографія. Основні принципи захисту інформації при підключенні до мережі Інтернет (виконання та захист лабораторної роботи № 8 на основі лекційного матеріалу та матеріалів лабораторних занять – 5 балів).

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

Підсумковий контроль (**залік**) – 40 балів: здійснюється виконання фінальної контрольної тестової роботи на курсі https://moodle.chnu.edu.ua/course/view.php?id=1357. **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 «Захист інформації в комп'ютерних системах».

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. Захист інформації в комп'ютерних системах : конспект лекцій / укл.: Іванущак Н.М. Чернівці : Чернівецький національний університет імені Ю. Федьковича, 2022. – 82 с.
2. Захист інформації в комп'ютерних системах: методичні вказівки до лабораторних робіт / укл.: Іванущак Н.М. Чернівці : Чернівецький національний університет ім. Ю. Федьковича, 2022. – 52 с.
3. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Львів: Новий світ-2000, 2020. – 678 с.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Чернівці: «Родовід», 2014. – 428 с.
5. Євсеєв С.П., Король О.Г., Шматко О.В. Кібербезпека: криптографія з PYTHON. Львів: Новий світ-2000, 2021. – 120 с.

Допоміжна

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.
2. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. – К.: Вид. ДУІКТ, 2009. – 292 с.
3. Беззубов Д.О. Суспільна безпека (організаційно-правові засади забезпечення): монографія / Д.О. Беззубов. – Київ : «МП Леся», 2013. – 425 с.
4. Данільян О.Г. Національна безпека України: структура та напрямки реалізації : [навч. посібник] / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Х. : Фоліо, 2002. – 285 с.
5. Жарков Я.М. Кібербезпека особистості, суспільства, держави : підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. — К. : Видавничо-поліграфічний центр Київський університет», 2008. – 256 с.
6. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. / Б.А. Кормич. – К. : Кондор, 2008. – 382 с.

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=1357