НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС

з дисципліни

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

для підготовки бакалаврів за спеціальністю 125 «Кібербезпека»

КИЇВ-2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від «17» травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

Спеціальність	125 - Кібербезпека
Освітня програма	Кібербезпека
Факультет	інформаційних технологій
Розробник:	Сагун А.В., к.т.н., доцент

Київ – 2023

1. Опис навчальної дисципліни

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	Кібербезпека	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2	
Семестр	3	
Лекційні заняття, год.	45	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	45	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	6 (15 тижнів)	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: ознайомлення з основними фізичними принципами, методами та засобами захисту інформації та пошуку розвідувальної апаратури, надання студентам знань з основ захисту інформації, принципів, методів та засобів несанкціонованого одержання інформації, а також створення протидії захисту інформації по каналах, на яких можливі її втрати.

Завдання навчальної дисципліни: полягає у вивченні засобів та методів захисту цілісності, конфіденційності та доступності інформації. Для чого розглядається використання криптографічних, інженерно-технічних, організаційних та мережевих методів та засобів захисту.

В результаті вивчення навчальної дисципліни студент повинен

знати:

- алгоритми створення проектів інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;
- принципи застосування теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- принципи застосування різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
- основи теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- принципи забезпечення введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
- алгоритми виявлення небезпечних сигналів технічних засобів.

вміти:

- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме:

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 12. Розробляти моделі загроз та порушника.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 19. . Застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітньо-професійної програми «Кібербезпека» першого (бакалаврського)рівня вищої освіти за спеціальністю 125 «Кібербезпека».
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Методи та засоби захисту інформації» є курси «Інформаційна безпека держави», «Теорія інформації та кодування», «Програмування», «Комп'ютерна логіка» ОПП першого (бакалаврського) рівня вищої освіти .

3. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Комп'ютерні методи і засоби захисту інформації													
Тема 1. Вступ до курсу. Причини, види та канали витоку інформації. Еволюційний розвиток методів та засобів захисту інформації (ЗІ).	1	5	2		3		-						
Тема 2. Методи та засоби захисту інформації, їх класифікація. Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту	2	10	2		4		4						
Тема 3. Захист властивостей інформації при передавання в комп'ютерних мережах. Захист цілісності з використанням алгоритмів підрахунку контрольних сум Ethernet-пакетів	2	20	4		4		8						
Тема 4. Моделювання вторгнення внаслідок несанкціонованого доступу. Моделі загроз та порушника.	3	2	2		-		-						
Тема 5. Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС	4	18	4		6		8						
Тема 6. Система електронного документообігу з точки зору кібербезпеки. Захист документаційної інформації та системи електронного документообігу, які підлягають захисту. Роль та функції ЕЦП в захисті.	5	14	6		8		-						
Разом за змістовим модулем 1		**69**	**20**		**25**		**20**						
Змістовий модуль 2. Організаційні та інженерно-технічні методи та засоби захисту інформації													
Тема 7. Психологічні засоби захисту інформації. Соціальна інженерія та методи боротьби з психологічними методами атаки на властивості інформації	6	2	2		-		-						
Тема 8. Методи захисту віддаленого доступу до інформації. Організація захищених з'єднань	7	8	4		4		-						
Тема 9. Налаштування авторизації до хмарних сховищ електронних	8	14	4		-		10						

документів. Спеціалізовані засоби захисту конфіденційності													
Тема 10. Методи забезпечення мережевої безпеки в КС. Мережеві сканери. Використання мережевих сканерів для фіксації втручання в роботу ІКС	10	8	4		4		-						
Тема 11. Налаштування систем блокування та попередження вторгнень (IDS та IPS системи). Міжмережеві екрани	11	20	4		4		12						
Тема 12. Реалізація та проектування політик безпеки/доступу в інформаційних системах	13	20	4		4		8						
Тема 13. Управління доступом та система реєстрації подій. Журналювання та аналітика безпеки	15	19	5		4		10						
Разом за змістовим модулем 2		**91**	**25**		**20**		**40**						
Всього годин		**150**	**45**		**45**		**60**						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Політика безпеки в ОС Linux. Власники і права доступу	3
2	Налаштування 2-факторної автентифікації в Linux UBUNTU	4
3	Дослідження технологій захисту цілісності інформації. Механізм контрольних сум. Алгоритму типу CRC та їх використання в мережевих протоколах Ethernet	4
4	Мережеві сканери. Використання мережевих сканерів для фіксації втручання в роботу ІКС	4
5	Створення моделі порушника інформаційної безпеки. Визначення та фіксація загроз ІБ	6
6	Дослідження технологій захисту цілісності та конфіденційності інформації (хешування). ЕЦП та її використання для захисту документаційної інформації	4

7	Налаштування системи авторизації та доступу для системи електронного документообігу (ЕДО) google docs (G-suite)»	4
8	Організація захищеного з'єднання протоколом ssh з віддаленим web-ресурсом	4
9	Налаштування систем блокування та попередження вторгнень. Міжмережеві екрани	4
10	Політики безпеки. Аудит подій безпеки	4
11	Безпека функціонування ОС	4
	Разом за семестр	**45**
	Разом	**45**

Курсове проектування - Не передбачено робочим навчальним планом

6. САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

– систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

– систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;

– сумлінну підготовку до лабораторних занять;

– вчасне і якісне оформлення звітів про лабораторні роботи.

6.1 Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Ядро ОС Linux та налаштування безпеки ядра ОС	8
2	Дослідження схем ЕЦП	4
3	Вивчення інженерних засобів протидії витокам інформації	8
4	Технологія створення вірусного ПЗ типу Trojan та боротьба з ним	10
5	Дослідження схем та протоколів автентифікації в ІКС	12
6	Системи визначення та блокування загроз (IDS та IPS))	8
7	Засоби аналізу та модифікації цілісності системного реєстру Windows	10

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

7.1. Питання для перевірки знань студентів:

1. Поняття інформації та його інтерпретації в законодавстві України (ЗУ «Про інформації»).

2. Властивості інформації, що підлягають захисту.

3. Методи та засоби захисту інформації, їх класифікація. Фізичні, апаратні, організаційні, програмні, законодавчі та психологічні засоби захисту.

4. Математичні (криптографія), технічні та інженерні засоби захисту інформації. Засоби їх реалізації. Програмна та апаратна реалізація методів та засобів захисту інформації.

5. Поняття відкритої інформації, інформація з обмеженим доступом та її види. Нормативно-правове обґрунтування.

6. Апаратні засоби захисту інформації. Реалізація криптографічних методів захисту (хешування та шифрування) в апаратних засобах ІКС.

7. Програмно – організаційні засоби захисту інформації в ОС.

8. Статистично-сигнатурні методи та засоби захисту інформації в ІКС. Антивірусні програми та сканери.

9. Засоби та методи здійснення атак на конфіденційності інформації. Механізми захисту конфіденційності. Парольний захист інформації та особливості його реалізації.

10. Засоби та методи здійснення атак на цілісність інформації. Механізми захисту цілісності.

11. Механізми авторизації та їх конструювання. Властивості інформації, що захищаються авторизацією.

12. Поняття етапної та факторної авторизації та приклади реалізації.

13. Ідентифікація та авторизація. Поняття ідентифікатора та механізм доведення автентичності. Приклади.

14. Методи та засоби захисту цілісності інформації. Механізми розрахунку та перевірки контрольних сум для мережевих пакетів та файлової інформації.

15. Методи та засоби захисту доступності інформації. Реплікація та back-up.

16. Поняття мережевої комп'ютерної безпеки. Засоби та методи гарантування захищеності основних властивостей інформації в комп'ютерних мережах.

17. Механізми збирання доказів кібернетичних втручань. Мережеві сканери. Відповідальних за здійснення та спроби здійснення кібератак та їх відображення в нормативно-правових актах України.

18. Механізми захисту файлових ресурсів та логіка розмежування доступу до файлових ресурсів в ОС Windows та Linux.

19. Політики безпеки. Засоби створення, редагування та імпортування локальних політик безпеки та механізмів аудиту безпеки.

20. Поняття «електронний підпис» та «електронний цифровий підпис», «електронна печатка» та їх роль у захисті різних властивостей інформації.

21. Електронний цифровий підпис. Роль та види ключів в схемах ЕЦП. Поняття центрів сертифікації ключів (ЦСК) та акредитації ЦСК (АЦСК). Нормативно-правове регулювання ЦСК та АЦСК.

22. Електронний документ та його роль в системі електронного документообігу (СЕДО). Засоби та методи захисту електронного документообігу.

23. Електронний документ та його реквізити. Механізми захисту електронного документу та його властивостей.

24. Основні складники СЕДО. Хмарні СЕДО. Методи та засоби захисту хмарний СЕДО.

25. Організація захисту віддаленого доступу до інформації в комп'ютерних мережах. Протоколи передавання інформації, захищені протоколи та методи захисту віддаленого телекомунікаційного з'єднання.

26. Криптографічні алгоритми захисту віддаленого телекомунікаційного з'єднання.

27. Атаки та інформацію типу «соціальна інженерія». Методи та засоби здійснення атак. Захист інформації від атак типу «соціальна інженерія».

28. Захист інформаційних систем та мереж. Міжмережеві екрани (МЕ) та їх функції. Особливості налаштування МЕ для захисту властивостей інформації.

29. Системи запобігання та визначення вторгнень. Їх функції та компоненти.

7.2. Приклади тестових питань з дисципліни:

Під методом захисту інформації розуміють:

- a. Метод захисту інформації, який дає похибки при захисті її властивостей
- b. Сукупність кроків, які потрібно здійснити, щоб виконати задачу або досягти мети щодо захисту певної властивості інформації
- c. Алгоритм проектування комплексної системи захисту інформації
- d. Назва будь-якої з властивостей інформації, що захищається
- e. Поняття, тотожне криптографічному захисту

Які права на доступ до файлу можуть мати користувачів, які не мають облікових даних авторизації google?

- a. Можуть мати той рівень права, який їм надав адміністратор сервісу google drive, на якому зберігається даний файл у відповідному посиланні
- b. Ні за яких умов вони не мають жодних прав, щодо доступу до файлу
- c. Тільки права на коментування файлу
- d. Можуть мати той рівень права, який їм надав створювач файла у відповідному посиланні
- e. Тільки права на перегляд файлу

8. Методи навчання

Виконання лабораторних робіт з використанням ПЗ Kleopatra, GP4Win, Linux Ubuntu, Cain@Abel, WireShark виконання індивідуальних навчально-дослідних завдань.

9. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

– на лабораторних роботах шляхом перевірки підготовки до виконання роботи;

– роботу над індивідуальними завданнями до лабораторних робіт;

– вивчення літератури, що рекомендувалася, та конспекту лекцій;

– оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

– на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;

– на лекційних заняттях виконується вибіркове опитування студентів;

– шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

10. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

11. Методичне забезпечення

1. Конспект лекцій з курсу "Методи та засоби захисту інформації ". - Київ, НУБіП, 2021 (https://elearn.nubip.edu.ua/course/view.php?id=3970)

12. Рекомендована література

Основна

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.

2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.

3. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510

4. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.

7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.

8. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

9. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

10. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

Додаткова

1. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

2. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю. Кондратьєва. – К., 2004.

3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

Інформаційні ресурси

1. https://elearn.nubip.edu.ua/course/view.php?id=3970
2. www.securityfocus.com.
3. www.sysinternals.com.
4. http://zakon1.rada.gov.ua