Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

" 31" 08 2024 р.
.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека»
(шифр і назва галузі знань)

Освітня програма: «Безпека інформаційних і комунікаційних систем»
(найменування освітньої програми)

Освітня програма «Кібербезпека»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Пєвнєв В.Я., професор, д.т.н., доцент. _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри _____
«Комп'ютерних систем, мереж і кібербезпеки»_____
(назва кафедри)

Протокол №1 від «30» 08 2024 р.

Завідувач кафедри д.т.н., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4.5(4)</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 Кібербезпека
(код та найменування)

Освітня програма
"Безпека інформаційних та комунікаційних систем"
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Кількість модулів –2</td><td colspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td colspan="2">2024/ 2025</td></tr>
<tr><td>Індивідуальне завдання РР</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин
денна – 112 / 255</td><td>7-й</td><td>8-й</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 4(3)
самостійної роботи студента – 4.5(5.5)</td><td colspan="2">Лекції 1)</td></tr>
<tr><td>32 годин</td><td>24 годин</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 годин</td><td>24 годин</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>71 годин</td><td>72 годин</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td>іспит</td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 112/143

.

2. Мета та завдання навчальної дисципліни

Мета – ознайомлення тих, хто навчається, з методологією, основними напрямами, методами і алгоритмами реалізації функцій захисту інформації від руйнівних програм в інформаційно-комунікаційних системах, а також придбанні навичок розробці та використання стенографічних алгоритмів щодо забезпечення захисту інформації.

Завдання:

– вивчити основні поняття, критерії та показники ефективності захисту інформації в інформаційно-комунікаційних системах;

– вивчити основні методи та засоби захисту інформації від руйнівних і шкідливих програм в інформаційно-комунікаційних системах;

– вивчити методи і засоби знаходження вразливостей та протидії атакам складовим інформаційно-комунікаційних систем;

– вивчити методи і засоби використання стеганографічних алгоритмів щодо забезпечення конфіденціальності в інформаційно-комунікаційних системах;

– оволодіти практичними навичками використання систем захисту інформації під час передавання та збереження інформації в інформаційно-комунікаційних системах.

Компетентності, які набуваються.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

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

ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН 12 Розробляти моделі загроз та порушника.

ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

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

ПРН 20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН 27 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН 53 Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Пререквізити – "Архітектура комп'ютерів", "Моделі та структури даних", "Апаратні та програмні засоби захисту інформації", "Інформаційно-комунікаційні системи", "Операційні системи".

Кореквізити –"Кваліфікаційна робота бакалавра".

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1.

Тема 1. Захист програм та даних

Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Характеристика сучасного стану проблематики в галузі забезпечення захисту інформації в інформаційних і комунікаційних системах та мережах.

Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку РПЗ. Методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ

Типи шкідливого ПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів.

Протидія і виявлення троянських програм, черв'яків та вірусів. Основи роботи антивірусних программ. Сигнатурний аналіз. Евристичні аналізатори. Поведінкові блокатори. Протидія шкідливому коду. Шкідливе ПЗ для мобільних пристроїв.

Захист програмного забезпечення. Ідентифікація програм та захист авторських прав

Тема 2. Захист в операційних системах**.**

Механізми захисту операційних систем Підсистема безпеки операційної системи та виконувані нею функції. Реалізація підсистем безпеки у найбільш розповсюджених операційних системах. Критерії захищеності операційних систем

Операційна система iOS. Операційна система Android. Операційна система Windows Phone. Операційна система BlackBerry.

Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи

Переповнення буферу. Поняття стеку та купи. Функції стеку викликів. Сегментація пам'яті. Причини виникнення переповнення буферу. Захист від переповнення буферу. Запобігання виконання даних.

Змістовий модуль 2.

Тема 3. Захист в мережах

Методи та засоби реалізації загроз в комп'ютерних системах та мережах. Загальні поняття (загроза, вразливість, атака, несанкціонована дія, порушник). Класифікація порушників і типів засобів реалізації загроз. Класифікація загроз безпеки інформації, що передається по мережі. Класифікація способів порушення автентичності суб'єктів та даних. Потенційні можливості порушення захищеності даних, що передаються по інформаційних каналах.

Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій. Засоби захисту локальних мереж при приєднанні до Інтернету. Технологія міжмережних екранів Технологія віртуальних приватних мереж. Методи та засоби захисту мобільного програмного забезпечення

Безпека веб-серверів та веб-застосувань. Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості. Тестування на вразливість до атак. Методика оцінки вразливостей. Тестування на вразливості. Сканери вразливостей. Послідовність дій при виконанні тестування веб-серверів та веб-застосувань на вразливість до атак згідно з OWASP.

Механізми DoS/DDoS атак. Об'єкти та види DoS атак. Захист від DoS/DDos атак.

Безпека в безпровідних мережах. Збір інформації про безпровідні мережі. Шифрування та автентифікація в безпровідних мережах. Атака на безпровідні мережі. Засоби захисту від безпровідних атак. Bluetooth

Модуль 2.

Змістовий модуль 3.

Тема 4. Захист в системах передачі даних та системах зв'язку

Методи та технології захисту інформації в системах передачі даних та системах зв'язку. Засоби захисту захист інформації в системах передачі даних та системах зв'язку. Організаційні засади забезпечення захисту інформації

Типи атак на систему передачі даних. Механізми захисту від атак. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Способи протидії пасивному збору інформації. Засоби активного сбору інформації про систему передачі даних. Пошук вразливостей та інструменти сканування вузлів систем передачі даних та систем зв'язку на вразливості. Оцінка захищеності інформації в системах передачі даних та системах зв'язку.

Механізми захисту від збору інформації, сканування та проникнення. Системи виявлення вторгнень та системи запобігання вторгненням.

Змістовий модуль 4.

Тема 5. Загальні відомості

Місце стеганографічних систем у сфері кібербезпеки. Терміни та визначення. Принципи побудови стеганографії. Структурна схема та математична модель типової стеганосистеми. Протоколи. Методи приховування інформації. Класифікація методів стеганографії. Класична стеганографія. Комп'ютерна стеганографія. Цифрова стеганографія. Мережева стеганографія. Цифрові водяні знаки.

Тема 6. Використання стеганографічних систем

Технологічна схема захисту. Приховування інформації в тексті. Методи довільного інтервалу. Синтаксичні та семантичні методи. Приховування даних в нерухомих зображеннях. Приховування даних в просторової області. Метод заміни найменш значущого біта. Метод псевдовипадкового інтервалу. Метод блокового приховування. метод квантування зображення. Приховування даних в частотної області зображення. Метод Коха і Жао. Метод Хсу і Ву. Метод Фрідріх. Методи розширення спектру. Статистичні методи. Структурні методи. Приховування даних в ауді сигналах. Кодування найменш значущих біт. Метод фазового кодування. Метод розширення спектра. Приховування даних з використанням луна - сигналу.

4. Структура навчальної дисципліни

Назви модулів і тем	Кількість годин				
	усього	у тому числі			
		л	п	лаб.	с.р.
Модуль 1					
Змістовий модуль 1.					
Тема 1. Захист програм та даних	33	8		8	17
Тема 2. Захист в операційних системах	34	8		8	18
Разом за змістовим модулем1	**67**	**16**		**16**	**35**
Змістовий модуль 2					
Тема 3. Захист в мережах		16		16	36
Разом за змістовим модулем 2	**68**	**16**		**16**	**36**
Разом за модулем 1	**135**	**32**		**32**	**71**

Модуль 2					
Змістовий модуль 3					
Тема 4. Захист в системах передачі даних та системах зв'язку.	36	8		8	20
Разом за змістовим модулем 3	**36**	**8**		**8**	**20**
Змістовий модуль 4					
Тема 5. Загальні відомості	26	6		4	16
Тема 6. Використання стегонографічних систем	58	10		12	36
Разом за змістовим модулем 4	**84**	**16**		**16**	**64**
Разом за модулем 2	**120**	**24**		**24**	**72**
Усього годин	**255**	**56**	**0**	**56**	**143**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	*Не передбачено*		
	Разом		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	*Не передбачено*		
	Разом		

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	2	3
1	Дослідження можливості виявлення вірусної активності вбудованими засобами ОС.	4
2	Дослідження можливості використання описаних вразливостей для вбудовування в вірусний код	4
3	Дослідження можливостей використання Metasploit для створення та відлагодження експлойтів.	4
4	Дослідження ефективності атак на парольний захист	4
5	Дослідження атаки типа «переповнення буферу» та методів протидії.	4

1	2	3
6	Дослідження методів пасивного та активного збору інформації про мережу.	4
7	Дослідження механізмів захисту мережі від збору інформації, сканування та проникнення	4
8	Дослідження алгоритмів завадостійкого кодування	4
9	Дослідження методів м'якого кодування	4
10	Порівняльний аналіз методів завадостійкого кодування	4
11	Дослідження цифрового водяного знаку	4
12	Дослідження можливостей розміщення повідомлення у текстовому файлі	4
13	Дослідження можливостей розміщення повідомлення у графічному файлі	4
14	Дослідження можливостей розміщення повідомлення у аудіо файлі	4
	Разом	**56**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку РПЗ. Методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ Типи шкідливого ПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів	17
2	Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи	18
3	Безпека веб-серверів та веб-застосувань. Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості. Тестування на вразливість до атак. Методика оцінки вразливостей. Тестування на вразливості. Сканери вразливостей. Послідовність дій при виконанні тестування веб-серверів та веб-застосувань на вразливість до атак згідно з OWASP.	36
4	Типи атак на систему передачі даних. Механізми захисту від атак. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Способи протидії пасивному збору інформації. Засоби активного сбору інформації про систему передачі даних. Пошук вразливостей та інструменти сканування вузлів систем передачі даних та систем зв'язку на вразливості. Оцінка захищеності інформації в системах передачі даних та системах зв'язку..	20

5	Класіфікація методів стеганографії. Класична стеганографія. Комп'ютерна стеганографія. Цифрова стеганографія. Мережева стеганографія. Цифрові водяні знаки	16
6	Статистичні методи. Структурні методи. Приховування даних в аудісігналах.Кодіроване найменш значущих біт. Метод фазового кодування. Метод розширення спектра. Приховування даних з використанням луна - сигналу.	36
	Разом	**143**

9. Індивідуальні завдання

Виконання РР (Оцінка вразливостей)

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, модульного контролю (тести за кожною темою), підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Робота на лекціях	0…1	16	0…16
Виконання і захист лабораторних робіт	0...5	8	0...40
Модульний контроль	0…22	2	0…44
Усього за семестр			**0 …100**
Модуль 2			
Робота на лекціях	0…1	16	0…16
Виконання і захист лабораторних робіт	0...5	8	0...40
Модульний контроль	0…22	2	0…44
Усього за семестр			**0…100**

Лабораторна робота має бути здана протягом двох тижнів. Для отримання максимальної оцінки повіни здати протягом трьох днів з моменту виконання за розкладом занять; 4 – 6; 3 – 9; 2 – 12; 1-14 днів

Участь у конференції -10 балів.

Стаття у фаховому журналі -20 балів

Критерії оцінювання знань студента під час іспиту

Задовільно (60-74). Захистити не менше 85% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних

та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування СТЗІ.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 95% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо розвитку та підтримки функціонування СТЗІ. Мати необхідний обсяг умінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти їх застосовувати. Уміти виконувати інформаційне забезпечення СТЗІ.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Презентації лекцій.
2. Керівництво до лабораторних робіт .
3. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.
4. Дистанційний курс в системі дистанційного навчання Ментор, розташований за адресою: https://mentor.khai.edu/course/view.php?id=4835.

14. Рекомендована література

Базова

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем._ К.: Вид.група BHV, 2009.-608 с.
2. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб.
3. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
4. Захист інформації в автоматизованих системах управління: навч. посіб. /Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

5. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020 . – 678 с

Допоміжна

6. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.

7. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/ 4

8. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/

9. Open Web Application Security Project [Електронний ресурс]. Режим доступу: a. www.owasp.org 6. Когут Ю.І. Кібербезпека

Інформаційні ресурси

10. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс]. – http://dstszi.gov.ua/

11. Офіційний сайт Google, на якому розміщена документація по работі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/appengine

12. 2. Офіційний сайт Microsoft, на якому розміщена документація по роботі із платформою Microsoft Azure. [Електронний ресурс].