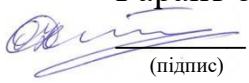
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2024 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації: проектування, впровадження, супровід
(назва навчальної дисципліни)

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

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

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

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Брежнєв Є.В. професор кафедри 503, д.т.н., проф.
(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 2022 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, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="9">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td rowspan="2">Навчальний рік
2024/2025</td></tr>
<tr><td>Кількість змістових модулів – 2</td></tr>
<tr><td>Індивідуальне завдання: не має</td><td rowspan="2">Семестр: 7</td></tr>
<tr><td>Загальна кількість годин – 64/120</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 3,5</td><td>Лекції [1)]32 год.</td></tr>
<tr><td>Практичні – не має</td></tr>
<tr><td>Лабораторні[1)] 32 год.</td></tr>
<tr><td>Самостійна робота 56 год.</td></tr>
<tr><td>Індивідуальні завдання: не має</td></tr>
<tr><td>Вид контролю: модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 64/120.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета діяльності: є формування у студентів теоретичних знань та практичних навичок у галузі проектування, впровадження та експлуатації комплексних систем захисту інформації; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів.

Завдання (ОК 28): застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні дані та обирати методи оцінки якості.

Компетентності, які набуваються. Дисципліна має допомогти сформувати у студентів такі компетентності.

Загальні компетентності

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.

Фахові компетентності.

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

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, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні 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 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

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 12 Розробляти моделі загроз та порушника.

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

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 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 19 Застосовувати теорії та методи 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 23 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

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

ПРН 33 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

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

ПРН 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

Пререквізити

Дисципліна базується на: ОК15 «Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах», ОК23 «Прикладна криптологія», ОК24 «Надійність та функціональна безпека інформаційно-управляючих систем», ОК25 «Системи технічного захисту інформації». Дисципліна є базовою для: ВБ1.7 «Комплексні системи захисту інформації: проектування, впровадження, супровід», ВБ1.15 «Комплексні системи захисту інформації: проектування, впровадження, супровід (КП)», ОК36 «Дипломний робота (проект) бакалавра».

Кореквізити - відсутні

3. Програма навчальної дисципліни

Змістовний модуль 1. Основи теорії захисту інформації.

ТЕМА 1. Вступна

Визначення комплексної системи захисту інформації. Етапи побудови КСЗІ. Принципи побудови КСЗІ.

ТЕМА 2. Архітектура безпеки ІТС

Загрози безпеки для ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС.

ТЕМА 3. Моделі захисту інформації

Визначення суб’єктів та об’єктів в моделях ЗІ. Мандатні моделі ЗІ. суб’єктно-об’єктні моделі ЗІ.

ТЕМА 4. Моделювання впливу на інформацію

МБО. МБС. ІПС. Ядро безпеки.

ТЕМА 5. Системи фізичного захисту об'єктів критичної інфраструктури

Критична інфраструктура. Категоризація об’єктів критичної інфраструктури. Особливості задач охорони об'єктів. Принципи забезпечення безпеки. Завдання систем захисту. Приклади.

ТЕМА 6. Визначення інформації яка потребує захисту.

Методика визначення інформації яка потребує захисту. Класифікація інформації. Проблеми визначення інформації.

ТЕМА 7. Визначення вартості інформації

Проблема визначення вартості інформації. Економічні методики визначення вартості інформації. Методика Дж. Кантера.

ТЕМА 8. Особливості об’єктів захисту

Категорії об’єктів захисту. Особливості охорони різних типів об’єктів. Структура системи забезпечення безпеки об’єктів.

Модульний контроль.

Змістовний модуль 2. Канали витоку інформації. Засоби контролю.

ТЕМА 9. Побудова комплексної системи охорони периметру **важливого об'єкту**

Загальні принципи забезпечення безпеки об’єктів. Системи охоронно-тривожної сигналізації. Охоронні сповіщувачі. АРМ охоронної системи.

ТЕМА 10. Аудит інформаційної безпеки

Аудит інформаційної безпеки (мета, завдання, класифікація). Види аудиту. Основні етапи аудиту безпеки

ТЕМА 11. Система контролю та управління доступом

Класифікація СКУД. Призначення СКУД. Електронна прохідна. Датчики СКУД.

ТЕМА 12. Системи телевізійного спостереження

Визначення та призначення. Класифікація. Відеокамери. АРМ системи відео нагляду.

ТЕМА 13. Системи пожежної сигналізації

Визначення та призначення. Класифікація. Сповіщувачі. Оповіщувачи. Система автоматичного пожежогасіння.

ТЕМА 14. Канали контролю доступу. Засоби контролю

Визначення та призначення. Зони охорони. Оптимізація побудови охорони периметру. Системи охорони периметру.

ТЕМА 15. Аспекти соціальної інженерії в КСЗІ

Концепції соціальної інженерії. Техніки соціальної інженерії. Соціальна інженерія у соціальних мережах. Крадіжка особистих даних. Контрзаходи соціальної інженерії

ТЕМА 16. Підсумок вивченого матеріалу

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Основи теорії захисту інформації.					
Тема 1. Вступ до дисциплини	2	2			
Тема 2. Архітектура безпеки ІТС	4	2			
Тема 3. Моделі захисту інформації	6	2		4	
Тема 4. Моделювання впливу на інформацію	18	2		6	10
Тема 5. Системи фізичного захисту об'єктів критичної інфраструктури	2	2			
Тема 6. Визначення інформації яка потребує захисту	12	2			10
Тема 7. Визначення вартості інформації	18	2		6	10
Тема 8. Особливості об’єктів захисту	2	2			
Разом за змістовним модулем 1	62	16		16	30
Усього годин за модуль 1	62	16		16	30
Модуль 2					
Змістовний модуль 2. Канали витоку інформації. Засоби контролю.					
Тема 9. Побудова комплексної системи охорони периметру важливого об'єкту	6	2		4	
Тема 10. Аудит інформаційної безпеки	7	2			5
Тема 11. Система контролю та управління доступом	7	2			5
Тема 12. Системи телевізійного спостереження	7	2			5
Тема 13. Системи пожежної сигналізації	7	2			5
Тема 14. Канали контролю доступу в промислових об’єктах для забезпечення безпеки	16	2		8	6
Тема 15. Аспекти соціальної інженерії в КСЗІ	2	2			
Тема 16. Підсумок вивченого матеріалу	2	2			
Разом за змістовним модулем 2	60	16		16	26
Усього годин за модуль 2	60	16		16	26
Усього годин за дисципліною	120	32		32	56

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Визначення вартості інформації	4
2	Вивчення моделей аналізу кібер інцидентів, загроз та правопорушника	4
3	Ознайомлення з програмними засобами (ПЗ) аналізу ризиків ІБ. Вивчення SecurITree	4
4	Визначення показника ефективності засобів охорони (ЗО) території об'єктів	4
5	Застосування інструментальних засобів для оцінювання ІБ комплексного промислового об’єкту	8
6	Застосування штучного інтелекту для розробки специфікації системи фізичного захисту об’єктів	8
	Разом	**32**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Теорія захисту інформації. Моделі захисту інформації	6
2	Архітектура безпеки інформаційно-телекомунікаційних систем	6
3	Параметричні канали витоку інформації	6
4	Система пожежної охорони як частина КСЗІ	6
5	СКУД. Принципи побудови та використання.	6
6	Вивчення можливостей програмного засобу моделювання загроз MS Threat Modeling tool	6
7	Методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	6
8	Особливості моніторингу процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки	6
9	Вивчення вимог нормативно-правових документів щодо побудови комплексних систем захисту інформації в автоматизованих системах (АС) організації (підприємства)	4
10	Огляд засобів щодо захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами.	4
	Разом	**56**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

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

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти
12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	7	0…7
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	3	0...18
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…25	1	0…25
Змістовий модуль 2			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	7	0…7
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	3	0...18
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…25	1	0…25
Усього за семестр			**0…100**

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Захистити всі індивідуальні завдання та здати тестування.

Добре (75 – 89). Твердо знать мінімум знань, виконати всі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основний та додатковий матеріал. Знати всі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

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

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: httpshttps://mentor.khai.edu/course/view.php?id=3718, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

- робоча програма дисципліни;
- конспект лекцій (презентації), в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;
- журнал успішності.
- Посилання на практики

14. Рекомендована література

Базова

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

2. Хорошко В. О. та ін Проектування комплексних систем захисту інформації - Л.: Львівська політехніка, 2020. - 320с

3. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин, 2019. – 144 с.

Допоміжна

1. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41 yaremchuk _kompleksni_systemy_zahystu_informaciyi/index.html

2. Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems / Thomas L. Norman

3. Physical Security Systems Handbook: The Design and Implementation of Electronic Security systems / Michael Khairallah

15. Інформаційні ресурси

1. Вадим Гребенніков Комплексні системи захисту інформації. Проектування, впровадження, супровід [Электрон. ресурс]. - Режим доступа: https://www.academia.edu/40525032/Комплексні_системи_захисту_інформації_проектування_впровадження_супровід

2. Microsoft IT Academy Program [Электрон. ресурс]. - Режим доступа: https://itacademy.microsoftelearning.com/

3. Cisco Networking Academy [Электрон. ресурс]. - Режим доступа: https://www.netacad.com/, http://www.cisco.com/web/learning/netacad/