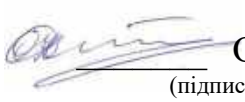
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми


Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно – комунікаційних системах

(назва навчальної дисципліни)

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

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

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

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025 року

Харків 2025 – р.

Розробник: Лисицький К.Є., ст.викладач, p.h.d., _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____
«Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол №_1_ від «_29_» _08_ 2025 р.

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

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Лисицький Костянтин Євгенійович

Посада: ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки

Науковий ступінь: p.h.d

Вчене звання: старший викладач

Перелік дисциплін, які викладає: Прикладна криптологія, Захист інформації в ІКС, Управління кібербезпекою

Напрями наукових досліджень: криптографічні алгоритми, симетрична криптографія, методи диференційного, лінійний, алгебраїчного криптоаналізу

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	*8*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС / кількість годин	*Денна:* 4 *кредита / 120 годин (48 аудиторних, з яких: лекції – 24, лабороторні – 24, СРЗ - 72)*
Види навчальної діяльності	*Лекції, лабораторні заняття, самостійна робота здобувача*
Види контролю	*Поточний контроль, модульний контроль, семестровий контроль – іспит*
Пререквізити	*"Вища математика", "Дискретна математика", "Теоретичні основи криптології".*
Кореквізити	*"Організація та безпека баз даних", "Побудова та кібербезпека інтернету речей", "Захист інформації в інформаційно-комунікаційних системах", "Комплексні системи захисту інформації: проектування, впровадження, супровід", " Кваліфікаційна робота бакалавра"*

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – Мета: здатність аналізувати методологію створення, основні напрями, методи, алгоритми реалізації функцій захисту інформації в інформаційно-комунікаційних системах, засоби забезпечення основних вимог інформаційної безпеки.

Завдання: знати сучасні міжнародні та вітчизняні стандарти з інформаційної безпеки; знати загальні аспекти проблематики в галузі інформаційної безпеки, а також тенденції і перспективи створення механізмів захисту інформації та засобів подолання цих механізмів; розуміти властивості інформаційних ресурсів та технологій, як об'єктів кібербезпеки, та вміння здійснювати класифікацію загроз безпеці інформаційних ресурсів, класифікацію та ранжирування джерел загроз і уразливостей безпеці, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; - розуміти принципи і методи теорії захищених систем, основних механізми захисту, яш реалізовані в сучасних операційних системах та системах управління базами даних, видів і прийомів використання шкідливого програмного забезпечення та методів його нейтралізації.

Компетентності, які набуваються:

***Інтегральна компетентність*:** Здатність розв'язувати складні спеціалізовані задачі та практичні проблема у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

***Загальні компетентності (КЗ)*:**

- КЗ1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ2. Знання та розуміння предметної області та розуміння професії.
- КЗ3. Здатність 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 спеціальності (КФ)*:**

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

Програмні результати навчання (ПРН):

- ІПР 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.
- ІПР 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.
- ІПРН 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.

4. Зміст навчальної дисципліни

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.

Тема лекції 1: Предмет, мета вивчення і задачі дисципліни. Характеристика сучасного стану проблематики в галузі забезпечення захисту інформації в інформаційних і комунікаційних системах та мережах.

Тема лекції 2: Руйнуючі програмні засоби (РПЗ).Типи шкідливого ПЗ.

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

Тема лекції 3: Захист в операційних системах**.**

Тема лабораторного заняття 1. Дослідження можливості виявлення вірусної активності вбудованими засобами ОС
Тема лабораторного заняття 2. Дослідження можливості використання описаних вразливостей для вбудовування в вірусний код.
Тема лабораторного заняття 3. Дослідження можливостей використання Metasploit для створення та відлагодження експлойтів.
Самостійна робота: опрацювання навчально-методичних матеріалів. Формування питань до викладача (онлайн-консультація).

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.
Тема лекції 4: Методи та засоби реалізації загроз в комп'ютерних системах та мережах.
Тема лекції 5: Засоби забезпечення безпеки в обчислювальних мережах. Захист серверів та робочих станцій. Безпека веб-серверів та веб-застосувань.
Тема лекції 6: Механізми DoS/DDoS атак. Об'єкти та види DoS атак. Захист від DoS/DDos атак.
Тема лабораторного заняття 4. Дослідження ефективності атак на парольний захист.
Тема лабораторного заняття 5. Дослідження атаки типа «переповнення буферу» та методів протидії.
Тема лабораторного заняття 6. Дослідження методів пасивного та активного збору інформації про мережу.
Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача.

Модульний контроль 1.

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 інформації в системах передачі даних та системах зв'язку. Організаційні засади забезпечення захисту інформації
Тема лекції 7: Типи атак на систему передачі даних. Механізми захисту від атак.
Тема лекції 8: Оцінка захищеності інформації в системах передачі даних та системах зв'язку. Механізми захисту від збору інформації, сканування та проникнення.
Тема лекції 9: Системи виявлення вторгнень та системи запобігання вторгненням.

Тема лабораторного заняття 7. Дослідження механізмів захисту мережі від збору інформації, сканування та проникнення.
Тема лабораторного заняття 8. Дослідження алгоритмів завадостійкого кодування
Тема лабораторного заняття 9. Порівняльний аналіз методів завадостійкого кодування
Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача

Змістовий модуль 4.

ТЕМА 5. Місце стеганографічних систем у сфері кібербезпеки. Терміни та визначення. Принципи побудови стеганографії.
Тема лекції 10: Структурна схема та математична модель типової стегосистеми.
ТЕМА 6. Використання стеганографічних систем**.**
Тема лекції 11: Технологічна схема захисту. Приховування інформації в тексті.
Тема лекції 12: Приховування даних в частотної області зображення. Метод Коха і Жао. Метод Хсу і Ву. Метод Фрідріх. Методи розширення спектру. Статистичні методи. Структурні методи.
Тема лабораторного заняття 10 Дослідження можливостей розміщення повідомлення у текстовому файлі
Тема лабораторного заняття 8. Дослідження можливостей розміщення повідомлення у графічному файлі
Тема лабораторного заняття 9. Дослідження можливостей розміщення повідомлення у аудіо файлі
Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача
Модульний контроль 2.

5. Методи навчання

Словесні, наочні, практичні; пояснювально-ілюстративні, репродуктивні, частково-пошукові; перевірки та оцінювання знань, умінь і навичок, усного викладу знань, закріплення навчального матеріалу, самостійної роботи з осмислення й засвоєння нового матеріалу.

6. Методи контролю

Проведення поточного контролю, електронного тестування, модульного контролю, підсумкового контролю у вигляді іспиту.

7. Критерії оцінювання та розподіл балів, які отримують здобувачі

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Виконання і захист лабораторних робіт	0...5	6	0...30
Модульний контроль	0…20	1	0…20
Змістовий модуль 2			
Виконання і захист лабораторних робіт	0...5	6	0...30
Модульний контроль	0…20	1	0…20
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.
Сумарна кількість балів не може бути більшою за 100.

Семестровий контроль у вигляді іспиту проводиться у разі відмови здобувача від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 30+30+40 балів.

Критерії оцінювання знань студента під час іспиту

Задовільно (60-74). Мати уявлення про принципи побудови симетричних (блочних і потокових) криптографічних алгоритмів та протоколів, що використовуються для забезпечення конфіденційності та автентичності і цілісності повідомлень, криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового), а також проводити порівняльний аналіз крипостійкості симетричних криптографічних систем.

Добре (75-89). Твердо знати характеристику методів і засобів криптографічного перетворення інформації, показники ефективності криптографічних систем, методи забезпечення автентичності користувачів комп’ютерної мережі, виконувати криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового) шифрування.

Відмінно (90-100). Мати теоретичні знання та практичні навички щодо побудови та використання систем шифрування та обміну ключами.

Таблиця 8.2 – Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою
	Іспит
90 – 100	Відмінно
75 – 89	Добре
60 – 74	Задовільно
0 – 59	Незадовільно

8. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі, які за певних обставин не можуть регулярно відвідувати лабораторні заняття, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після пропуску. Здобувачі, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Дотримання вимог академічної доброчесності. Під час вивчення навчальної дисципліни здобувачі мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

9. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки та у системі дистанційного навчання «Ментор».

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu .

2. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL https://mentor.khai.edu/course/view.php?id=2165.

11. Рекомендована литература

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 світ-2000», 2020 . – 678 с.
6. Костюк Ю. В., Складанний П. М., Бебешко Б. Т. та ін. «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 2025).

Допоміжна:

1. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
2. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/ 4
3. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
4. Open Web Application Security Project [Електронний ресурс]. Режим доступу: a. www.owasp.org 6. Когут Ю.І. Кібербезпека

Інформаційні ресурси

1. http://dstszi.gov.ua/
2. Офіційний сайт Google, на якому розміщена документація по роботі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/appengine

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