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

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

ЗАТВЕРДЖУЮ
Гарант освітньої програми

О. Ілляшенко
(підпис) (ініціали та прізвище)
« 29 » серпня 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою
(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)

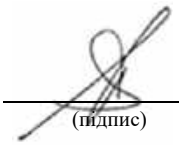
Силабус введено в дію з 01.09.2025 року

Харків 2025 рік

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	*7*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС / кількість годин	*Денна: 4 кредити / 120 годин (48 аудиторних, з яких: лекції – 32, лабороторні – 16, СРЗ - 72)*
Види навчальної діяльності	*Лекції, лабораторні заняття, самостійна робота здобувача*
Види контролю	*Поточний контроль, модульний контроль, семестровий контроль – залік*
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 навчальної дисципліни: діяльності на основі застосування системи теоретичних знань і практичних навичок: формування комплексу засобів (правил, процедур, тощо) щодо управління інформаційною безпекою; застосування комплексного підходу з забезпечення інформаційної безпеки в різних сферах діяльності (критичні системи та додатки).

Завдання: знати структуру нормативних актів та стандартів в сфері управління інформаційної безпекою; систему термінів та понять; організовувати основні процеси реалізації систем ІБ, а саме, планування, ризик-аналізу, вибору контрзаходів, тощо; ВМ1ТИ використовувати сучасні інформаційні технології при оцінювання ризиків критичної інфраструктури; визначати шляхи зниження ризиків, практично застосовувати методи забезпечення безпеки.

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)*:**

- 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 проблема за професійним
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
- КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

***Фахові компетентності спеціальності (КФ)*:**

- КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
- КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

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

- ІПРН 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.
- ІПРН 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 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.
- 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).
- ПНР 25 Забезпечувати 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.
- 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 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно- телекомунікаційних систем.
- ПРН 32 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
- 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 41 Забезпечувати неперервність процесу ведення журналів реестрації подій та інцидентів на основі автоматизованих процедур.
- ПРН 42 Впроваджувати процеси виявлення, ідентифжації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
- ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
- ПРН 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризишв та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
- ПРН 45 Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-оріснтованому контролі доступу до інформаційних активів.
- ПРН 46 Здійснювати аналіз та мінімізацію ризишв обробки інформації в інформаційно- телекомунікаційних системах.

- ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
- ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно- телекомунікаційних системах.

4. Зміст навчальної дисципліни

Змістовий модуль 1

Тема 1. Аудит інформаційної безпеки. Види аудиту. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 ТА ISO 19011. Комплексний аудит.
Тема лекції 1: Вступ до дисципліни. Аудит інформаційної безпеки. Види аудиту. Принципи аудиту.
Тема лекції 2: Розробка звіту про аудит.
Тема лекції 3: Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 ТА ISO 19011.
Тема лекції 4. Комплексний аудит інформаційної системи.
Тема лабораторного заняття 1. Дослідження стандартів CobiT, ITIL, ISO/IEC 15408, ISO/IEC 270XX.
Тема лабораторного заняття 2. Дослідження принципів комплексного аудиту інформаційної системи.
Самостійна робота: здобувачів опрацювання навчально-методичних матеріалів. Формування питань до викладача (онлайн-консультація).

Тема 2. Управління інцидентами інформаційної безпеки**.** Приклади вразливостей. Реагування на інциденти.

Тема лекції 5: Базові принципи, терміни та визначення.
Тема лекції 6: Стандарт ISO/IEC 27001.
Тема лекції 7: Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки.
Тема лекції 8: Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.
Тема лабораторного заняття 3 Розробка опитувальника (інструмент аудитора)..
Тема лабораторного заняття 4. Розробка бланку для фіксації результатів внутрішнього аудиту та протоколу відхилень.
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 2.

Тема 3. Приклади вразливостей, які можуть бути використані для реалізації відповідних загроз для комерційної структури. Функціонування груп діяльності груп CERT/CSIRT.

Тема лекції 9: Вразливості, які можуть бути використані для реалізації

відповідних загроз для комерційної структури
Тема лекції 10: Етапи створення груп CERT/CSIRT.
Тема лекції 11: Обробка інцидентів інформаційної безпеки групами CERT/CSIRT.
Тема лекції 12: Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

Тема лабораторного заняття 5. Дослідження системи менеджменту інформаційної безпеки.
Тема лабораторного заняття 6. Дослідження стандарту ISO/IEC 27004:2009.

Тема 4. Методичні підходи до розробки політики інформаційної безпеки підприємства.
Тема лекції 13: Політика безпеки інформації.
Тема лекції 14: Методичні підходи до розробки політики інформаційної безпеки підприємства.
Тема лекції 15: Порядок розробки політики.
Тема лекції 16: Робоча група для розробки політики інформаційної безпеки.
Тема лабораторного заняття 7 Дослідження кращих практик політики інформаційної безпеки в Україні.
Тема лабораторного заняття 8 Дослідження кращих практик політики інформаційної безпеки в європейських країнах.
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, підсумковий контроль у вигляді заліку.

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	4	0...20
Модульний контроль	0…30	1	0…30
Змістовий модуль 2			
Виконання і захист лабораторних робіт	0...5	4	0...20
Модульний контроль	0…30	1	0…30
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 більш 100.

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

Білет для заліку 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
	Залік
90 – 100	Відмінно (зараховано)
75 – 89	Добре (зараховано)
60 – 74	Задовільно (зараховано)
0 – 59	Незадовільно (незараховано)

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=4255 .

10. Рекомендована литература

Базова:

1. European Network and Information Security Agency (ENISA) [Електронний ресурс] // Режим доступу: http:// www.enisa.europa.eu.

2. Guidelines for auditing management systems : ISO 9011:2011 // International Organization for Standardization (ISO). – 2011. – 52 p.

3. Системи захисту інформації : підручник / Ю. Костюк, П. Складаний, Г. Гулак та ін. — Київ : Київський столичний університет імені Бориса Грінченка, 2025. — 887 с. — URL: elibrary.kubg.edu.ua

4. Кібербезпека і управління інформаційними ресурсами : навчальний посібник. — Київ : Юрінком Інтер, 2025. — URL: jurkniga.ua

5. Cybersecurity: Technology and Governance / ed. by Springer Nature. — 2025. — URL: link.springer.com

Допоміжна:

1. Інформаційна безпека: нові виклики та стратегії захисту // Науковий вісник Ужгородського національного університету. Серія: Право. — 2025. — Вип. 60, ч.2.-URL: visnyk-juris-uzhnu.com

2. Кібербезпека: інформаційно-аналітичний дайджест № 10/2025 / НБУВ. — 2025.-URL: https://ippi.org.ua/sites/default/files/2025-10_0.pdf

3. Управління ризиками кібербезпеки за методологією NIST : практичний гайд. — 2025. — URL: visuresolutions.com

11. Інформаційні ресурси

1. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс] – http://dstszi.gov.ua.
2. КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ, МЕРЕЖ І КІБЕРБЕЗПЕКИ [Електронний ресурс] – http://www.csn.khai.edu.
3. Стандарт ISO/IEC27001- [Електронний ресурс] - https://www.iso.org/standard/27001