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)

«29» серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇНАВЧАЛЬНОЇ 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)

Рівень вищої освіти:***перший (бакалаврський)***

Силабус введено в дію з 01.09.2025 року

Харків – 2025р.

Розробник:  Брежнєв Є.В., проф., д.т.н
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

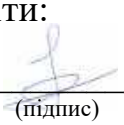
Силабус розглянуто на засіданні кафедри

комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » 08 2025 р.

Завідувач кафедри д.т.н., професор  ВячеславХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я таПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:


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

1. Загальна інформація про викладача

Брежнєв Євген Віталійович
професор кафедри комп'ютерних систем, мереж і кібербезпеки
доктор технічних наук, професор
Викладає дисципліни: «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Методи дослідження комп'ютерних систем та мереж», «Технології бізнес аналітики».
Напрями наукових досліджень: застосування інформаційних технологій щодо побудови захисту складних технічних систем, методи забезпечення гарантоздастності систем що базуються на штучному інтелекті, безпека критичних інфраструктур.
Контактна інформація:
e-mail: e.brezhnev@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	8 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	4,5 кредити ЄКТС / 135 годин (48 аудиторних, з яких: лекції – 24, практичні роботи – 24, самостійна робота – 87)
Види навчальної діяльності	Лекції, практичні заняття.
Види контролю	Модульний контроль, семестровий контроль – іспит
Пререквізити	«Захист інформації в інформаційно-комунікаційних системах», «Прикладна криптологія», «Надійність та функціональна безпека інформаційно-управляючих систем», «Системи технічного захисту інформації».

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

Мета: є формування у здобувачів освіти 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:

– вивчити основні поняття комплексної системи захисту інформації;

– 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:

а) 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

б) 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:

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».

4. Зміст навчальної дисципліни

Змістовний модуль 1. Захист інформації інформаційно-телекомунікаційних мережах.

ТЕМА 1. Захист інформації в обчислювальних мережах

Загрози обчислювальним мережам. Методи захисту мереж. Механізми забезпечення безпеки.

Тема Лекції 1: «*Захист інформації в обчислювальних мережах*».

ТЕМА 2. Засоби резервного копіювання інформації в мережах

Огляд сучасних тенденцій резервного зберігання даних. Огляд систем резервного копіювання.

Тема Лекції 2: «*Засоби резервного копіювання інформації в мережах*».

Тема практичної роботи 1: Розробка методу порівняльної оцінки захищеності систем електронного документообігу

ТЕМА 3. Місце IP-адреси в системі захисту конфіденційної інформації.

IP-протокол та його версії. Веб-браузер та його місце у правопорушеннях. Способи виявлення прихованої IP-адреси.

Тема Лекції 3: «*Місце IP-адреси в системі захисту конфіденційної інформації*».

ТЕМА 4. Побудова захищених локальних мереж.

Принципи побудови захищених локальних мереж. Фізичне розділення мережі. VPN мережі. Захищенні оптичні локальні мережі.

Тема Лекції 4: «*Побудова захищених локальних мереж*».

Тема практичної роботи 2:Основи використання VPN

ТЕМА 5. Захист системи відеоспостереження

Структура та основні елементи. Основні параметри камер відеоспостереження. Пристрої обробки відеосигналів. Методи захисту систем відео спостереження.

Тема Лекції 5: «***Захист системи відеоспостереження***».

ТЕМА 6. Побудова комплексної системи охорони периметру.

Аналогові системи. Цифрові системи. Комбіновані системи. Пересилання пакетів. Шлюзи. Принципи побудови захищеної мережі відео нагляду, охоронно-тривожної сигналізації, контролю та керування доступом.

Тема Лекції 6: «*Побудова комплексної системи охорони периметру: системи охороно-тривожної сигналізації* ».

Тема Лекції 7&8: «*Побудова комплексної системи охорони периметру: системи контролю та керування доступом та відео спостереження*

Модульний контроль

Змістовний модуль 2. Методи та засоби протидії зловмисникам в комп'ютерних мережах.

ТЕМА 7. Методи контролю доступу до ОТ в КСЗІ

Вразливості парольного захисту. Корпоративна парольна політика. Захист доступу до ОТ за допомогою електронних брелоків та старт карт. Засоби біометричного захисту до ОТ.

Тема Лекції 9: «Методи контролю доступу до ОТ в КСЗІ».

Тема практичної роботи 3: Програмна реалізація резервного копіювання даних

ТЕМА 8. Брандмауери

Програмні та апаратні брандмауери, принципи реалізації. Принципи реалізації та використання брандмауерів в ОС Windows. Принципи реалізації та використання брандмауерів в ОС Linux, MacOS.

Тема Лекції 10: «Брандмауери».

ТЕМА 9. Використання мереж стільникового зв'язку для скоєння правопорушень

Характеристика стільникового зв'язку. Стандарти стільникового зв'язку. Методи захисту мереж стільникового зв'язку.

Тема Лекції 11: «Аспекти інформаційної безпеки щодо використання стільникового зв'язку».

Тема практичної роботи 4: Вивчення програмних утиліт контролю доступу до інформаційних ресурсів

Тема 10. Методи фільтрації спаму

Характеристика спаму та осіб що його відправляють. Ризики спаму. Типи спаму. Засоби боротьби зі спамом. Фільтр Байєса. Оновлення чорних списків. Сірі списки. Переваги на недоліки.

Тема практичної роботи 5: Отримання практичних навичок з аудіті безпеки комп'ютерної мережі

Тема Лекції 12: «Методи фільтрації спаму ».

Модульний контроль.

5. Індивідуальні завдання

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

6. Методи навчання

Словесні (пояснення, розповідь, проблемний виклад), наочні (ілюстрування, демонстрація, презентація), практичні.

7. Методи контролю

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

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1,2			
Виконання і захист лабораторних робіт	0…5	3	0…15
Модульний контроль	0…25	1	0…25
Змістовий модуль 3,4			
Виконання і захист лабораторних робіт	0...5	5	0…25
Виконання і захист розрахунково-графічного завдання	0...10	1	0…10
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

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

Білет для іспиту складається із двох теоретичних та одного практичного запитання, максимальна кількість балів за кожне теоретичне запитання, складає 34 балів, а за практичне – 32 балів.

Таблиця 2 – Шкали оцінювання: бальна та традиційна

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

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи. Знати основні поняття щодо захисту інформації в обчислювальних мережах. Розуміти загрози обчислювальним мережам та основні методи захисту мереж. Механізми забезпечення безпеки. Знати основні засоби резервного копіювання інформації в мережах та місце IP-адреси в системі захисту конфіденційної інформації. Розуміти вразливості веб-браузеру та його місце у правопорушеннях. Способи виявлення прихованої IP-адреси. Знати принципи побудови захищених локальних мереж, принципи фізичного розділення мережі. Вміти аналізувати вимоги до комплексної системи захисту, виходячи з вимог технічних завдань на розроблення системи; розраховувати показники ефективності, базуючись на основних методах та програмному забезпеченні систем з використанням відповідних методів оцінювання.

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. Окрім знать, необхідних для отримання задовільної оцінки, здобувач освіти повинен знати основні принципи побудові *захисту системи відеоспостереження.* Розуміти структуру та основні елементи та методи захисту систем відео спостереження. Розуміти основи *побудови комплексної системи охорони периметру*. Принципи побудови захищеної мережі відео нагляду, охороно-тривожної сигналізації, контролю та керування доступом. Вміти формулювати вимоги до комплексної системи захисту; розраховувати показники ефективності, базуючись на основних методах. Вміти будувати архітектуру безпеки інформаційної системи.

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 роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах. Окрім знань, необхідних для отримання оцінки добре, здобувач освіти повинен знати методи контролю доступу до ОТ в КСЗІ. Знати основні вразливості парольного захисту, основні принципи побудови корпоративної парольної політики. Методи вибору засобів доступу до ОТ за допомогою електронних брелоків та старт карт. Розуміти програмні та апаратні брандмауери, принципи реалізації. Розуміти принципи реалізації та використання брандмауерів в ОС Windows. Знати особливості використання мереж стільникового зв'язку для скоєння правопорушень, методи захисту мереж стільникового зв'язку. Знати методи фільтрації спаму.

Вміти формулювати вимоги до комплексної системи захисту та використовувати методи розробки таких систем.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Характер курсу передбачає необхідність відвідування занять. Здобувачі освіти, які за певних обставин не можуть відвідувати заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувані освіти 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 освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувана освіти 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/).

10. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1609

11. 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

12. 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/