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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Дмитро УЗУН
(підпис) ім'я та ПРІЗВИЩЕ)

« 31 » серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Технології розроблення та забезпечення функційної безпечності ІКС»
(назва навчальної дисципліни)

Галузь знань: F Інформаційні технології
(шифр і найменування галузі знань)

Спеціальність: F5 Кібербезпека та захист інформації
(код та найменування спеціальності)

Освітня програма: Кібербезпека та захист інформації
(найменування освітньої програми)

Рівень вищої освіти: другий (магістрський)

Силабус введено в дію з 01.09.2025 року

Харків – 2025 р.

Розробник: Вдовіченко О. О., доцент каф. 503, д-філ (PhD). _____
(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 _____ Вячеслав ХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Представник здобувачів освіти:
_____ _____ Іван ОЛЕФІРЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Вдовіченко Олександр Олександрович

Посада: доцент

Науковий ступінь: доктор філософії (PhD)

Вчене звання: -

Перелік дисциплін, які викладає:

- Надійність та відмовостійкість КС;
- Безпека індустріальних систем та IoT;
- Вбудовані радіоелектронні системи на основі ПЛІС;
- Технології розроблення та забезпечення функційної безпечності ІКС.

Напрями наукових досліджень:
системи Інтернету речей, розумні пристрої, надійність та відмовостійкість обчислювальних систем, методи оптимізації побудови і взаємодії технічних рішень, автоматизація та робототехніка.

Контактна інформація:
o.vdovichenko@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	1 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна:* 4 кредити ЄКТС / 120 годин (СРЗ – 120)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	Дисципліна є обов'язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.
Кореквізити	Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін: ОК8 «Методи та технології кібербезпеки критичних інфраструктур», ОК9 «Стандартизація і сертифікація систем кібербезпеки»

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

Мета – надати студентам знання і навички із забезпечення безпеки ІКС, вбудованих систем та засобів, що формують IoT інфраструктуру.

Завдання:

– придбання знань про базові поняття з функціональної безпеки;

– придбання знань про основи управління функціональною безпекою та життєвим циклом ІКС;

– придбання знань про основи кількісного оцінювання функціональної безпеки та розрахунку показників функціональної безпеки;

– придбання знань про основи технічних та організаційних заходів забезпечення функціональної безпеки;

− отримання практичних знань з оцінювання різних функціональної безпеки, можливих ризиків, що можуть виникати в процесі експлуатації ІКС та розроблення стратегії їх модернізації.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

ЗК1. Здатність до адаптації та дій в новій ситуації.

ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.

ЗКЗ. Здатність проводити дослідження на відповідному рівні.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

Спеціальні компетентності:

СК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технологій створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

СК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

СК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

СК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

СК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

СК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

СК11. Здатність аналізувати і розробляти методи і засоби оцінювання та забезпечення функційної безпечності інформаційно-керуючих систем.

Програмні результати навчання:

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технологій, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ПРН24. Аналізувати та оцінювати показники функційної безпечності інформаційно-керуючих систем та обґрунтовувати рекомендації щодо її забезпечення відповідно вимогам нормативних документів.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. Основи аналізу функціональної безпеки

Тема 1. Загальні відомості про функціональну безпеку ІКС

Стисла анотація: Тенденції розвитку ІКС у контексті глобальної ініціативи «Індустрія 4.0». Архітектура існуючих ІКС: «Інтернет речей», автоматизовані системи управління технологічними процесами (АСУ ТП),

вбудовані системи, програмовані логічні контролери (ПЛК). Задачі забезпечення інформаційної та функціональної безпеки при зрощенні технологій «Інтернет речей» та АСУ ТП. Ризики експлуатації ІКС. Джерела ризиків та приклади порушень функціональної безпеки. Властивості ІКС. Головні атрибути інформаційної та функціональної безпеки. Структура вимог до інформаційної та функціональної безпеки.

Тема 2. Вимоги стандартів щодо функціональної безпеки ІКС

Огляд стандартів з інформаційної та функціональної безпеки ІКС. Стандарт МЕК 61508 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою». Зв'язки між частинами МЕК 61508 та короткий зміст частин. Систематизація вимог до інформаційної та функціональної безпеки. Приклади успішної сертифікації контролерів щодо вимог МЕК 61508

Тема 3. Менеджмент функціональної безпеки

Порівняння менеджменту інформаційної та функціональної безпеки. План керування функціональною безпекою. План керування персоналом. План керування конфігурацією. Керування зміненнями. Вибір та оцінювання програмних засобів розробки. План верифікації та валідації. План документування та структура документів з функціональної безпеки. Оцінювання та аудит функціональної безпеки.

Тема 4. Життєвий цикл інформаційної та функціональної безпеки

Поняття життєвого циклу. Повний життєвий цикл та життєвий цикл розробки. V-образний життєвий цикл. Етап «Концепція». Етап «Вимоги». Етап «Архітектурний проект». Етап «Проект програмного забезпечення». Етап «Проект технічних засобів». Етап «Кодування програмного забезпечення». Етап «Тестування програмного забезпечення». Етап «Інтеграційне тестування». Етап «Валідація». Етап «Введення до експлуатацій». Етап «Експлуатація та супроводження». Етап «Зняття з експлуатації». Планування життєвого циклу.

Змістовний модуль 2. Основи забезпечення функціональної безпеки

Тема 5. Оцінювання функціональної безпеки

Структура атрибутів інформаційної та функціональної безпеки. Підхід до аналізу ризиків ІКС та встановлення рівнів інтегрованості функціональної безпеки. Зв'язок показників надійності та функціональної безпеки. Інтенсивності безпечних та небезпечних, діагностовних та недіагностовних відмов. Середня імовірність небезпечної відмови за запитом функції безпеки. Середня частота небезпечних відмов функції безпеки. Доля безпечних відмов. Діагностичне покриття. Вимоги до кількісних показників функціональної безпеки ІКС згідно IEC 61508. Методологія аналізу видів, режимів та критичності відмов (FMECA).

Оптимізація структури ІКС за показниками готовності та критерієм функціональної безпеки.

Тема 6. Методи забезпечення функціональної безпеки ІКС

Топологічні та конструктивні особливості ІУС. Типові програмно-апаратні рішення із забезпечення функціональної безпеки ІУС. Багатоканальні архітектури. Самодіагностування. Захист від зовнішніх впливів. Використання якісних компонентів. Принцип діверсності. Типові організаційні заходи із забезпечення функціональної безпеки ІУС. Управління проектами.

Тема 7. Управління вимогами до функціональної безпеки

Процес інженерії вимог. Ідентифікація та аналіз вимог. Верифікація і валідація вимог. Забезпечення якості вимог. Пряме та зворотне трасування вимог. Програмні засоби підтримки трасування вимог.

Тема 8. Методологія Assurance Case

Зміст та теоретичні основи методології Assurance Case. Формальна нотація CAE (Claim – Argument – Evidence). Формальна нотація GSN (Goal Structured Notation). Інтеграція методології Assurance Case у життєвий цикл ІУС. Програмні засоби підтримки методології Assurance Case.

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

Проведення консультацій, звітної конференції, а також самостійна робота студентів за матеріалами, опублікованими кафедрою (п.11, 12).

7. Методи контролю

Проведення поточного контролю з використанням системи електронного тестування кафедри комп'ютерних систем, мереж і кібербезпеки, підсумковий контроль у вигляді іспиту.

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

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			

Робота на лекціях	0…2	7	0…14
Виконання і захист лабораторних робіт	0...4	3	0...12
Модульний контроль	0…24	1	0…24
Змістовний модуль 2			
Робота на лекціях	0…2	7	0…14
Виконання і захист лабораторних робіт	0...4	3	0...12
Модульний контроль	0…24	1	0…24
Усього за семестр			**0…100**

Білет для іспиту складається з двох теоретичних питань (30 балів за кожне питання) та практичного завдання (40 балів).
Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна та 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

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять. Знати основи аналізу та забезпечення функціональної безпеки. Уміти оцінювати рівень функціональної безпеки ІКС.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять. Знати ключові принципи аналізу та забезпечення функціональної безпеки. Уміти застосовувати різні архітектури ІКС для забезпечення зданного рівню функціональної безпеки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти забезпечувати функціональну безпеку ІКС. Вміти застосовувати методологію Assurance Case.

9. Політика навчального курсу

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни, у тому числі 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 можуть бути розцінені як прояв академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача 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 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

Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор».

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3696

11. Рекомендована література

Базова

1. Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety [Text] / N. Leveson. – The MIT Press, 2011. – 534 p.
2. Smith, D. Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards [Text] / D. Smith, K. Simpson. – Elsevier Butterworth-Heinemann, Oxford, UK, 2004. – 263 p.
3. Medoff, M. Functional Safety – An IEC 61508 SIL 3 Compatible Development Process [Text] / M. Medoff, R. Faller. – exida.com L.L.C., Sellersville, PA, USA, 2010. – 281 p.
4. Basilio, A. Functional Safety of Safety–Related Systems. Manual for Plant Engineering and Maintenance [Text] / A. Basilio, F. Landrini, G. Novelli, G. Landrini, M. Baldrigh]. – G.M. International S.r.l, Villasanta, Italy, 2008. – 388 p.

Допоміжна

1. NIST SP 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). – National Institute of Standards and Technologies, 2015.
2. ABB Safety Handbook. Machine Safety – Jokab Safety products. – ABB, 2013.
3. Syllabus: REQB® Certified Professional for Requirements Engineering. Foundation Level, Version 2.1. – Requirements Engineering Qualification Board, 2014.
4. Standard glossary of terms used in Requirements Engineering, Version 1.3. – Requirements Engineering Qualification Board, 2014.
5. GSN Community Standard ,Version 1. – Origin Consulting (York) Limited, 2011.

12. Інформаційні ресурси

1. Публікації з кібербезпеки National Institute of Standards and Technologies [Електрон. ресурс] – Режим доступу: http://csrc.nist.gov/publications/ PubsSPs.html#SP 800/.
2. Асоціація підприємств промислової автоматизації України (АППАУ) [Електрон. ресурс] – Режим доступу: http://appau.org.ua/.