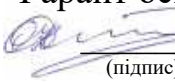
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

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

Апаратні та програмні засоби захисту інформації
(назва навчальної дисципліни)

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

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

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

Рівень вищої освіти: перший (бакалаврський)

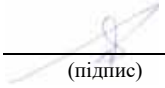
Силабус введено в дію з 01.09.2025 року

Харків – 2025 р.

Розробник: Перепелицин А.Є., доцент, к.т.н., доцент 
(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 » серпня 2025 року

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: *Перепелицин Артем Євгенович*

Посада: *доцент кафедри комп'ютерних систем, мереж і кібербезпеки*

Науковий ступінь: *кандидат технічних наук*

Вчене звання: *доцент*

E-mail: a.perepelitsyn@csn.khai.edu

Перелік дисциплін, які викладає*: Апаратні та програмні засоби захисту інформації, Дисципліна індивідуального вибору за фахом 2 (Кібербезпека апаратних засобів і сервісів), Технології забезпечення кібербезпеки апаратних та програмовних засобів.*

Напрями наукових досліджень: *архітектури обчислювальних систем, інтернет речей (IoT), хмарні технології, AI/ML*

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	*4*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС / кількість годин	*Денна: 3 кредита / 90 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16, СРЗ – 42)*
Види навчальної діяльності	*Лекції, лабораторні заняття, самостійна робота здобувача*
Види контролю	*Поточний контроль, модульний контроль, семестровий контроль – іспит*
Пререквізити	*"Архітектура комп'ютерів", "Операційні системи", "Технології проектування комп'ютерних систем", "Комп'ютерна електроніка і схемотехніка"*

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

Мета: формування фундаментальних знань на основі застосування системи теоретичних і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти, що застосовуються у складі апаратних засобів захисту інформації.

Завдання: оволодіння принципами побудови та вивчення основних закономірностей, методів та моделей засобів захисту інформації, можливість їх використання щодо захисту інформації, а також реалізація сучасних крипто алгоритмів на ПЛІС з використанням сучасних САПР як інструментального середовища розробники апаратних засобів безпеки.

Компетентності, які набуваються:

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК):

– ЗК1. Здатність застосовувати знання у практичних ситуаціях

– ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

– ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

– ЗК4. Здатність спілкуватися іноземною мовою.

– ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні компетентності (СК):

– СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

– СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

– СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

– СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

– СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

– СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

– СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

– СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно встановленою політикою інформаційної безпеки.

Результати навчання (РН):

– РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

– РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

– РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

– РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

– РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

– РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

– РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

– РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

– РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

– РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційнокомунікаційних системах відповідно до встановленої політики інформаційної безпеки.

– РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування

інформаційних й інформаційно-комунікаційних систем та або інфраструктури організації в цілому.

– РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

– РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації інформаційних системах;

– РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

– РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

– РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Засоби та технології реалізації генератора псевдовипадкових чисел в FPGA.

Тема 1. Технології реалізації генератора псевдовипадкових чисел в FPGA.

Предмет, ціль вивчення й завдання дисципліни. Структура, зміст дисципліни й методичні рекомендації з її вивчення. Місце дисципліни в навчальному процесі. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Технології реалізації генератора псевдовипадкових чисел в FPGA.

Тема 2. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.

Регістри зсуву з лінійної зворотним зв'язком. Конфігурації ГПСЧ на основі РЗЛЗЗ. Порівняння структури конфігурацій Фібоначі і Галуа. Переваги та недоліки конфігурацій Фібоначі і Галуа.

Тема 3. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.

Регістри зсуву з нелінійним зворотним зв'язком. порядок нелінійності поліномів. РЗНЗЗ другого порядка нелінійності. Поліноми, що утворюють структуру, для генерації послідовності макс. довжини.

Тема 4. Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.

Клітинні автомати. Класифікація клітинних автоматів. ГПСЧ на основі одновимірних клітинних автоматів. Розгляд різних правил для одновимірних клітинних автоматів.

Тема 5. Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA.

Оцінка якості формованих псевдовипадкових послідовностей. Реалізація криптостійких генераторів з використанням кріптопрімітівов.

Модульний контроль 1.

МОДУЛЬ 2
Змістовний модуль 2. Засоби та технології реалізації фізичної криптографії.

Тема 6. Генератори дійсно випадкових чисел.

Джерела ентропії. Апаратні реалізації генераторів істинно випадкових чисел. Генератор дійсно випадкових числових послідовностей в FPGA.

Тема 7. Реалізація фізично не клонованих функцій в FPGA.

Архітектури ФНФ. Поняття неклонованості. Властивості. Область застосування ФНФ. Протокол взаємодії. Оцінка якості реалізації ФНФ. Проблеми реалізації. Адаптація ФНФ для реалізації в FPGA.

Тема 8. Атаки по сторонніх каналах.

Атаки по сторонніх каналах. Фізичні характеристики, що лежать в основі атак по сторонніх каналах. Способи аналізу, що застосовуються в атаках по сторонніх каналах. Види атак по сторонніх каналах. Атаки по енергоспоживанню. Атаки за часом. Атаки за помилками обчислення. Атаки по електромагнітному випромінюванню. Атаки на основі акустичного аналізу. Атаки на кеш-пам’ять.

Тема 9. Апаратні трояни.

Класифікації апаратних закладок. Методи виявлення апаратних закладок. Заходи запобігання встановлення.

Тема 10. Обфускація і деобфускація FPGA.

Обфускація схем. Методи обфускації. Деобфускація схем. Фактори, що визначають застосовність обфускації. Оцінка ефективності обфускації схем.

Тема 8. Тригери. Класифікація тригерів. Типи тригерів. Синтез тригерів. Скінченні автомати. Синтез автоматів Мілі та Мура

Анотація: Тригери як елементна база апаратних генераторів псевдовипадкових послідовностей, регістрів зсуву та схем синхронізації в системах безпеки. Скінченні автомати як формальна модель для проектування апаратних протоколів автентифікації, керування доступом та детекторів аномальних станів на ПЛІС.

Модульний контроль 2

5. Індивідуальні завдання

Реалізація алгоритму шифрування AES в ПЛІС.

6. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів курсу (п.14, 15).

7. Методи контролю

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

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

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист лабораторних робіт	0…9	4	0…36
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0...9	4	0…36
Модульний контроль	0…10	1	0…10
Розрахунково-графічна робота	0...8	1	0…8
Усього за семестр			**0…100**

Під час складання семестрового іспиту здобувач освіти 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 балів за відповідь за кожне теоретичне питання та 40 балів за практичне.

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Виконати та захистити 75% лабораторних робіт та пройти 100% тестових завдань. Вміти аналізувати вимоги щодо проектування елементів/вузлів комп'ютерних обчислювальних систем. Вміти чітко визначати тип логіки що застосовується для розв'язання певного коло задач. Володіти знаннями в галузі існуючих методів, програмно-технічних засобів які використовуються в процесі проектування обчислювальних вузлів комп'ютерних систем.

Добре (75-89). Володіти необхідним мінімумом знань в галузі проектування комп'ютерних систем з використанням елементної бази ПЛІС. Об'єм знань має бути достатніми для самостійного розв'язання задач середньої складності. Виконати та захистити 85% лабораторних робіт та пройти 100% тестових завдань. Вільно володіти програмно-технічними та інструментальними засобами розроблення обчислювальних вузлів комп'ютерних систем, їх тестування та імплементація з використанням елементної бази ПЛІС. Розв'язувати завдання на високому рівні з використанням сучасних підходів до проектування та загальних рекомендацій.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконало володіти темами та вміти застосовувати на практиці отриманні знання. Допомагати одногрупникам в процесі оволодінням знаннями в рамках дисципліни.

Таблиця 8.2 – 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

9. Політика навчального курсу

Відвідування занять. Інтерактивний характер курсу передбачає обов’язкове відвідування лабораторних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати лабораторні 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 здобувачі 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. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів 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 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=4835

11. Рекомендована література

Базова

1. Матвієнко М. П., Розен В. П. Комп'ютерна схемотехніка. Навчальний посібник. – К.: Видавництво Ліра-К, 2020. – 192 с.
2. Азаров О. Д., Гарнага В. А., Клятченко Я. М., Тарасенко В. П. Комп'ютерна схемотехніка: підручник. – Вінниця: ВНТУ, 2018. – 230 с.
3. Схемотехніка: пристрої цифрової електроніки : електрон. підручник для вищих навчальних закладів Т. 1 / В. М. Рябенький, В. Я. Жуйков, Ю. С. Ямненко, А. В. Заграничний. – Київ : НТУУ КПІ, 2016. – 400 с.
4. Схемотехніка: пристрої цифрової електроніки : електрон. підручник для вищих навчальних закладів Т. 2 / В. М. Рябенький, В. Я. Жуйков, Ю. С. Ямненко, А. В. Заграничний. – Київ : НТУУ КПІ, 2016. – 358 с.

Допоміжна

1. Строкань О.В, Прийма С.М., Литвин Ю.О. Комп’ютерна схемотехніка та архітектура комп’ютерів: лабораторний практикум. – Мелітополь, 2019. – 186 с.

2. Основи прикладної теорії цифрових автоматів: підручник / І. А. Дичка, В. П. Тарасенко, М. В. Онай ; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 506 с.

3. Комп’ютерна схемотехніка: Навчальний посібник. – Луцьк: РРВ Луцького НТУ, 2016. – 236 с.

4. Paul Horowitz, Winfield Hill. The Art of Electronics 3rd Edition. 2015. – 1225 p. ISBN 978-0-521-80926-9

5. David M. Harris, Sarah L. Harris. Digital Design and Computer Architecture. Elsevier Inc. 2012. – 1684 p.

6. Introduction to Digital Systems Design. Donzellini Giuliano et all. 2018. Springer Publishing Company, Incorporated. ISBN: 978-3-319-92803-6.

7. A.P. Plakhtyeyev. E.V. Babeshko, V.A. Tkachenko, J.V. Zdorovets. Architectures and Embedded Platform Based development of Internet / Web of Things systems: Laboratory works / V.S. Kharchenko (edit.) - Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, 2019. – 147 p.

12. Інформаційні ресурси

1. Quartus II Web Edition Design Software – [Ел. ресурс]. – Режим доступу: https://www.intel.com/content/www/us/en/software-kit/711791/intel-quartus-ii-web-edition-design-software-version-13-0sp1-for-windows.html

2. ModelSim – Intel FPGA Edition Simulation Quick-Start – [Ел. ресурс]. – Режим доступу: https://cdrdv2-public.intel.com/666396/ug_gs_msa_qii-683248-666396.pdf