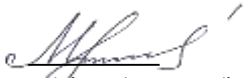
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми


(підпис) Ольга МОРОЗОВА
(ім'я та ПРІЗВИЩЕ)

«29» серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології забезпечення кібербезпеки апаратних та програмовних засобів
(назва навчальної дисципліни)

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

Спеціальність: F7 «Комп'ютерна інженерія»
(код і найменування спеціальності)

Освітньо-наукова програма: «Системне програмування»
(найменування освітньої програми)

Рівень вищої освіти: **другий (магістерський)**

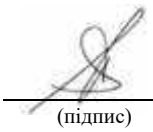
Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник: Перепелицин А.Є., доцент, к.т.н., доцент 
(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 2025р.

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

Погоджено з представником здобувачів освіти:


(підпис) Дмитро ВАСИК
(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

Перелік дисциплін, які викладає:
Апаратні та програмні засоби захисту інформації, 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

Контактна інформація:
a.perepelitsyn@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	3
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС / кількість годин	Денна: 4 кредити / 120 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16, СРЗ – 72)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота здобувача
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

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.

Завдання: оволодіння принципами побудови та вивчення основних закономірностей, методів та моделей засобів захисту інформації, можливість їх використання щодо захисту інформації, а також апаратна реалізація сучасних крипто алгоритмів з використанням сучасних середовищ розроблення.

Компетентності, які набуваються:

Загальні компетентності (ЗК):

ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.

Спеціальні компетентності (СК):

СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

Програмні результати навчання (ПРН):

ПРН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

ПРН9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Теоретичні аспекти технології забезпечення кібербезпеки апаратних та програмовних засобів.

Тема 1. Вступ до дисципліни

Стисла анотація: 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. Характеристика рекомендованих під час вивчення дисципліни джерел інформації.

Лабораторна робота № 1: Дослідження та розрахунок складності алгоритму зламу потенційної системи з застосування методів «грубої сили».

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція

Стисла анотація: Історія розвитку сучасних апаратних засобів для забезпечення кібербезпеки. Програмні та апаратні засоби захисту від кібератак. Загальна характеристика. Відмінності. Особливості застосування.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак

Стисла анотація: Класифікація апаратних засобів з точку зору забезпечення кібербезпеки. Апаратні комплекси як об'єкт кібератак. Програмовні та апаратні платформи для здійснення кібератак.

Лабораторна робота № 2: Аналіз потенційних загроз та дослідження уразливості апаратних та програмовних компонентів системи на прикладі одноплатного комп'ютеру Raspberry Pi.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів

Стисла анотація: Сучасні стандарти забезпечення кібербезпеки. Кібербезпека промислових систем управління. Стандарти ISA/IEC 62443. NERC-CIP. UL 2900-2-2.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів

Стисла анотація: Характеристика системи та ідентифікація загроз. Аналіз ризиків та загроз. Розрахунок ризиків та можливих впливів. Управління ризиками. Сучасні стандарти. ISO/IEC 27001.

Лабораторна робота № 3: Розробка апаратного комплексу аналізу проектних рішень комбінаційних та секвенційних схем з використанням програмовної логіки класу FPGA.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 6. Види та характеристика атак на електроні та програмовні компоненти

Стисла анотація: Таксономія та класифікація видів атак на електроні компоненти. Рівні атак, їх виявлення та аналіз післядії. Інвазивні, напівінвазивні та неінвазивні атаки. Особливості застосування. Класифікація програмовних компонентів та види атак. Атаки на електроні компоненти, в яких алгоритми виконуються програмно (мікроконтролери, мікропроцесори тощо). Атаки на апаратні компоненти з програмовною логікою (ПЛІС).

Самостійна робота: Опрацювання матеріалу лекцій.

Модульний контроль 1.

Змістовний модуль 2. Практичні аспекти забезпечення кібербезпеки апаратних та програмовних засобів.

Тема 7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти

Стисла анотація: Загальна характеристика та особливості застосування. Відмінності, методи виявлення та протидії. Неінвазивні атаки - атаки сторонніми каналами (Side-channel attacks). Напівінвазивні атаки - атаки на основі помилок обчислень (Fault Attacks). Інвазивні атаки - атаки засновані на фізичному втручанні (Physical tampering).

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 8. Атака сторонніми каналами

Стисла анотація: Класифікація видів атак. Пасивні та активні атаки. Атаки за рівнем доступу. Методи впливу та протидії. Атаки зондуванням (Probing Attack). Атаки по енергоспоживанню (Power Analysis Attack). Атаки по електромагнітному випромінюванню (electromagnetic Analysis). Акустичні атаки (Acoustic Attack). Атаки по видимому випромінюванню (Visible Light Attack).

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 9. Апаратні закладки (Trojans)

Стисла анотація: Загальна характеристика. Класифікація видів та рівнів внесення апаратних закладок. Класифікація по фізичному принципу роботи. Класифікація по методу активації. Класифікація по дії на систему. Оцінка потенційної загрози. Методи виявлення.

Лабораторна робота № 4: Розробка апаратного комплексу пошуку апаратних закладок з використанням програмовної логіки класу FPGA.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання

Стисла анотація: Рівні та проблеми несанкціонованого доступу. Засоби обмеження фізичного доступу до апаратних компонентів на різних рівнях. Захист від читання (Readout Protection). Захист процесу завантаження (Boot Flow Protection) та ініціалізації. Шифрування даних, що зберігаються.

Лабораторна робота № 5: Розробка обфускатору сирцевого коду для захисту його від несанкціонованого копіювання та зміни.

Самостійна робота: Опрацювання матеріалу лекцій.

Тема 11. Захист сирцевого коду від несанкціонованого копіювання, обфускатори

Стисла анотація: Реверс інжиніринг. Обфускатори сирцевого коду. Техніки обфускації. Особливості використання сторонніх бібліотек з точки зору безпеки. Цифрова підпис (GPG). Ізоляція процесів розробки як частина процесів Continuous Integration/Continuous Delivery.

Самостійна робота: Опрацювання матеріалу лекцій.

Модульний контроль 2

5. Індивідуальні завдання

Апаратна реалізація алгоритму шифрування.

6. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів курсу (п.11, 12).

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
Виконання індивідуального завдання	0...8	1	0…8
Усього за семестр			**0…100**

Під час складання семестрового іспиту студент 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 студента 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/user/index.php?id=1613

11. Рекомендована література

Базова

1. Forte, S. Bhunia, M M. Tehranipoor. Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment. – Springer, 2017. 349 p.
2. R. Paul. Secure Hardware Design: Services and Security. – VDM Verlag Dr. Mülle, 2010. 152 p.
3. D. Mukhopadhyay, R.S. Chakraborty. Hardware Security: Design, Threats, and Safeguards. – Chapman & Hall/CRC, 2014 – 542 p.
4. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник. – К.: Дуікт, 2010. 316 с.
5. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009.

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