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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми


(підпис) Дмитро Узун (ім'я та ПРІЗВИЩЕ)

«_31_» ____серпня____2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології DevSecOps
(назва навчальної дисципліни)

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

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

Освітньо-професійна програма: «Кібербезпека та захист інформації»
(найменування освітньої програми)

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

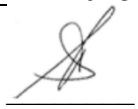
Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): Узун Д.Д., професор, к.т.н., доцент 
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » серпня 2025 р.

Завідувач кафедри д.т.н., професор  Вячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:


(підпис) Іван ОЛЕФІРЕНКО
(ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Узун Дмитро Дмитрович

Посада: професор

Науковий ступінь: кандидат технічних наук

Вчене звання: доцент

Перелік дисциплін, які викладає:

Домени кібербезпеки
Технології ДевСекОпс
Технології ДевОпс
Операційні системи
Безпека хмарних технологій
ДевОпс та хмарні технології

Напрями наукових досліджень:

Впровадження сучасних технологій автоматизації циклу розробки та забезпечення стану безпеки IT-проектів

Контактна інформація:

d.uzun@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	1
Мова викладання	Українська, англійська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	4 кредити ЄКТС / 120 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16; СРЗ – 72)
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

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

Мета дисципліни – формування у студентів теоретичних знань та практичних навичок з впровадження принципів DevSecOps - інтеграції безпеки у всі етапи життєвого циклу розробки програмного забезпечення (SDLC) із використанням сучасних інструментів DevOps та технологій кібербезпеки

Завдання:

Сформувати у студентів здатність:

- розуміти концепцію DevSecOps та принцип Shift Left Security
- будувати безпечні CI/CD пайплайни
- здійснювати SAST, DAST, SCA та аналіз IaC
- захищати контейнеризовані середовища (Docker / Kubernetes)
- безпечно керувати секретами
- проводити моніторинг та реагування на інциденти
- автоматизувати контроль безпеки

Компетентності, які набуваються:

Інтегральна компетентність:

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

Загальні компетентності (ЗК):

ЗК1. Здатність до адаптації та дій в новій ситуації.
ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК3. 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.
ЗК8. Здатність спілкуватися іноземною мовою.

Спеціальні компетентності (СК):

СК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у 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.
СК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
СК7. Здатність 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.
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.
СК12. Здатність аналізувати, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших IT-інфраструктур.

Програмні результати навчання (ПРН):

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 технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології 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.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки 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.
ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
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.
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.
ПРН25. Аналізувати, обґрунтовувати вибір, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1.

Тема 1. Вступ до дисципліни. Архітектура DevSecOps.

Стисла анотація:

Поняття та еволюція DevSecOps як підходу до безпечної розробки програмного забезпечення. Відмінності між DevOps та DevSecOps. Основні принципи DevSecOps: Shift Left, автоматизація безпеки, безперервний контроль. Архітектура DevSecOps-пайплайну. Ролі та відповідальність учасників процесу (Dev, Sec, Ops). Інтеграція безпеки на етапах CI/CD. Значення культури безпеки в життєвому циклі ПЗ.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з базовими поняттями DevOps та DevSecOps. Аналіз типового CI/CD-пайплайну з точки зору безпеки.

Тема 2. Git, GitHub та secure workflows.

Стисла анотація:

Призначення системи контролю версій Git у процесі розробки програмного забезпечення. Основні принципи роботи Git та GitHub. Архітектура репозиторіїв і моделі роботи з кодом (Git Flow, Trunk-based Development). Поняття secure workflows. Контроль доступу та управління правами. Використання pull request та code review як елементів безпеки. Захист репозиторіїв: секрети, токени, гілки, підпис комітів. Основні ризики при роботі з Git та способи їх мінімізації.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з базовими командами Git. Аналіз прикладів безпечної та небезпечної роботи з репозиторіями. Вивчення принципів secure workflow у GitHub.

Тема 3. Безпека CI/CD .

Стисла анотація:

Поняття CI/CD та його роль у сучасній розробці програмного забезпечення. Архітектура CI/CD-пайплайнів та їхні компоненти. Основні загрози безпеці в CI/CD (компрометація пайплайнів, витік секретів, небезпечні залежності, supply chain attacks). Принципи побудови безпечного CI/CD. Інтеграція засобів безпеки у pipeline (SAST, DAST, SCA, secret scanning). Управління доступами, секретами та артефактами. Логування, моніторинг і контроль змін у процесі автоматизованої доставки.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з типовою структурою CI/CD-конвеєра. Аналіз можливих вразливостей у процесі CI/CD. Вивчення підходів до інтеграції інструментів безпеки в CI/CD-конвеєрі.

Тема 4. Статичне та динамічне тестування безпеки застосунків (SAST, DAST).

Стисла анотація:

Поняття статичного (SAST) та динамічного (DAST) аналізу безпеки застосунків. Місце SAST і DAST у життєвому циклі розробки програмного забезпечення та в DevSecOps-пайплайні. Принципи роботи інструментів статичного аналізу коду. Особливості динамічного тестування вебзастосунків. Переваги та обмеження SAST і DAST. Типові вразливості, що виявляються (OWASP Top 10). Інтеграція SAST/DAST у CI/CD. Інтерпретація результатів сканування та зниження кількості хибнопозитивних спрацювань.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з принципами роботи SAST та DAST-інструментів. Аналіз прикладів виявлених вразливостей. Вивчення підходів до інтеграції тестування безпеки в CI/CD.

Тема 5. Аналіз безпеки компонентів ПЗ (SCA).

Стисла анотація:

Поняття аналізу безпеки компонентів програмного забезпечення (Software Composition Analysis, SCA). Роль open-source компонентів у сучасній розробці та пов’язані з ними ризики. Виявлення вразливих, застарілих і ліцензійно небезпечних залежностей. Робота з базами вразливостей (CVE, NVD). Поняття SBOM (Software Bill of Materials) та його значення для безпеки ланцюга постачання ПЗ. Інтеграція SCA в DevSecOps-пайплайн. Управління ризиками сторонніх бібліотек та контроль відповідності ліцензійним вимогам.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з принципами роботи SCA-інструментів. Аналіз прикладів уразливих залежностей у програмних проєктах. Вивчення ролі SBOM у забезпеченні безпеки програмного забезпечення.

МОДУЛЬ 2
Змістовний модуль 2.

Тема 6. Безпека контейнерів. Кубернетес.

Стисла анотація:

Поняття контейнеризації та її роль у сучасних DevSecOps-процесах. Архітектура контейнерних середовищ та основи роботи Docker. Основні загрози безпеці контейнерів. Безпечна побудова контейнерних образів. Контроль вразливостей у контейнерах. Основи безпеки Kubernetes: архітектура кластера, контроль доступу (RBAC), ізоляція ресурсів, безпека

мережевих взаємодій. Захист контейнеризованих застосунків у середовищі оркестрації. Інтеграція перевірок безпеки контейнерів у CI/CD.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з принципами безпечної роботи з контейнерами. Аналіз типових вразливостей контейнерних середовищ. Вивчення базових механізмів захисту Kubernetes та їх ролі в DevSecOps.

Тема 7. Забезпечення захисту хмарних ресурсів (IAC, Cloud Security)

Стисла анотація:

Поняття хмарних обчислень та моделей надання послуг (IaaS, PaaS, SaaS). Основні загрози безпеці хмарних середовищ. Принципи спільної відповідальності (Shared Responsibility Model). Infrastructure as Code як основа автоматизованого розгортання інфраструктури. Ризики безпеки при використанні IaC. Контроль конфігурацій, керування доступом і секретами в хмарних середовищах. Інструменти перевірки безпеки IaC. Захист хмарних ресурсів у DevSecOps-процесах.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з принципами безпечної роботи з хмарною інфраструктурою. Аналіз типових помилок конфігурації в хмарних середовищах. Вивчення ролі IaC у забезпеченні безпеки та відтворюваності інфраструктури.

Тема 8. Керування обліковими даними та ключами. Secret Management

Стисла анотація:

Поняття облікових даних і секретів у сучасних інформаційних системах. Типи секретів: паролі, токени, API-ключі, сертифікати. Основні загрози, пов’язані з витоком облікових даних. Принципи безпечного зберігання та обробки секретів. Централізовані системи керування секретами. Ротація, контроль доступу та аудит використання секретів. Інтеграція secret management у CI/CD та хмарні середовища. Запобігання витокам конфіденційних даних у DevSecOps-процесах.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з підходами до зберігання та захисту облікових даних. Аналіз типових помилок у роботі з секретами. Вивчення ролі систем керування секретами в безпечній розробці та експлуатації застосунків.

Тема 9. Моніторінг та SIEM

Стисла анотація:

Поняття моніторингу безпеки в сучасних інформаційних системах. Роль логування та збору подій у DevSecOps. Джерела подій безпеки: застосунки, сервери, мережеве обладнання, хмарні сервіси. Принципи роботи SIEM-систем. Кореляція подій та виявлення інцидентів безпеки. Основи побудови

правил детекції та алертингу. Значення моніторингу для своєчасного виявлення атак і реагування на інциденти. Інтеграція SIEM у DevSecOps-процеси.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з принципами збору та аналізу логів. Аналіз типових подій безпеки та сценаріїв їх виявлення. Вивчення ролі SIEM у забезпеченні безперервного контролю безпеки.

Тема 10. Реагування на інциденти.

Стисла анотація:

Поняття інциденту інформаційної безпеки та його життєвий цикл. Основні етапи реагування на інциденти: підготовка, виявлення, аналіз, локалізація, усунення та відновлення. Роль Threat Detection у DevSecOps. Методи виявлення загроз на основі сигнатур, поведінкового аналізу та аномалій. Використання журналів подій і телеметрії для розслідування інцидентів. Взаємодія команд Dev, Sec та Ops під час реагування на інциденти. Значення постінцидентного аналізу та покращення процесів безпеки.

Самостійна робота:

Опрацювання матеріалів лекції. Ознайомлення з етапами реагування на інциденти. Аналіз типових сценаріїв кіберінцидентів. Вивчення підходів до виявлення загроз та реагування на них у DevSecOps-середовищі

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

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

7. Методи контролю

Проведення поточного контролю, електронного тестування, підсумковий контроль 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…8	3	0…24
Модульний контроль	0…26	1	0…26
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0…8	3	0…24
Модульний контроль	0…26	1	0…26
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови здобувача освіти від балів підсумкового контролю й за наявності допуску до іспиту. Під час складання семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних запитань (максимальна кількість балів за кожне – 25), та практичного запитання (максимальна кількість балів – 25).

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74) – Показати мінімум знань та умінь. Захистити не менше 50% від усіх завдань лабораторних занять. Знати основні складові дисципліни. Уміти користуватись інструментальними засобами, що розглянуті в курсі.

Добре (75-89) – Знати та розуміти теоретичну частину, захистити не менше 75% завдань лабораторних занять. Знати ключові концепції кожного модуля курсу. Вміти обґрунтовано впроваджувати потрібні інструментальні засоби відповідно до поставленої задачі.

Відмінно (90-100) – Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Вміти обґрунтовано користуватись інструментальними засобами з метою їх інтеграції при проведенні комплексного дослідження стану кібербезпеки ІТ-рішень.

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

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=9543

11. Рекомендована література

Базова

1. Tarandach I., Coles M. Threat Modeling. A Practical Guide for Development Teams. O'Reilly, 2021. 208 p
2. Messier R. Learning Kali Linux. O'Reilly; 2024. 520 p
3. Hoffman A. Web Application Security. O'Reilly; 2024. 444 p
4. Berlin A., Brotherston L., Defensive Security Handbook. O'Reilly; 2024. 363 p
5. Armitage J. Cloud Native Security Cookbook. O'Reilly; 2022. 516 p

Допоміжна

1. Dotson C. Practical Cloud Security. O'Reilly; 2024. 231 p

12. Інформаційні ресурси

1. DevSecOps Learning Path. TryHackMe [Ел. ресурс]. URL: https://tryhackme.com/path/outline/devsecops
2. DevSecOps Tools (Codecademy) [Ел. ресурс]. URL: https://www.codecademy.com/learn/ext-courses/important-devsecops-tools
3. Introduction to Secure DevOps. Microsoft Learn [Ел. ресурс]. URL: https://learn.microsoft.com/uk-ua/training/modules/introduction-to-secure-devops/
4. Secure CI/CD Pipelines [Ел. ресурс]. URL: https://www.classcentral.com/course/youtube-devsecops-implementing-secure-ci-cd-pipelines-56756
5. OWASP Juice [Ел. ресурс]. URL: https://owasp.org/www-projects/juice-shop/