Силабус освітнього компонента

Програма навчальної дисципліни

Безпека в DEVOPS

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
5

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу» , «Безпека та аудит бездротових та рухомих мереж», гарант освітньо-професійної програми "Управління інформаційною безпекою" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

ГАВРИЛОВА Алла Андріївна

alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Вступ до спеціальності. Ознайомча практика», «Організаційне забезпечення захисту інформації», «Безпека в DevOps», «Організація та безпека баз даних», «Управління IT-проєктами та їх

безпека» у студентів бакалавріату
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека в DEVOPS" є вибірковою навчальною дисципліною. Дисципліна «Безпека в DEVOPS» присвячена вивченню методології DevSecOps на практичних прикладах та спрямовує навчання студентів на розуміння й застосування кращих підходів до забезпечення безпеки життєвого циклу програмного продукту (у більшості розглядаються веб-застосунки та ресурси хмарних обчислень).

Мета та цілі дисципліни

Формування системи теоретичних знань і набуття практичних умінь і навичок щодо забезпечення безпеки на протязі життєвого циклу існування веб-рішень, що виконуються на боці серверу; оволодіння навичками застосування сучасного програмного забезпечення щодо рішень завдань DevOps і набуття компетенцій з використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та кібербезпеки.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Розробка та аналіз алгоритмів, Фізичні основи технічних засобів розвідки, Інформаційна безпека держави, Математичні основи криптології, Введення в мережі, Технології програмування, Основи побудови та захисту мікропроцесорних систем, Менеджмент інформаційної безпеки, Основи математичного моделювання систем безпеки, Основи криптографічного захисту, Безпека в інформаційно-комунікаційних системах, Комплексні системи захисту інформації, Безпека інтернет-речей.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Особливості сучасних мов програмування та розробки веб-орієнтованих застосунків. Особливості розробки веб-застосунків. Налагодження середовища розробки. Відмінності платформ Windows, Linux та MacOS у якості середовища	2

розробника. Поняття гнучкого (Agile) управління розробкою програмних продуктів.	
Тема 2. Розгортання операційної системи Linux та Windows у якості платформи веб-сервера. Застосування скриптів для автоматизації процесів розгортання програмного забезпечення. Знайомство з технологіями Chef, Puppet та Ansible. Особливості забезпечення безпеки рівня операційної системи та веб-серверу.	2
Тема 3. Особливості технологій серверної віртуалізації. Визначення гіпервізору та контейнерної віртуалізації. Особливості роботи із системами управління віртуальними машинами. Особливості забезпечення безпеки рівня віртуальної машини.	2
Тема 4. Технології хмарних обчислень (Cloud Computing). Засоби автоматизації DevOps у хмарних середовищах на прикладах: Amazon AWS, Microsoft Azure та рішень Red Hat OpenShift. Особливості забезпечення безпеки рівня хмарного середовища.	2
Тема 5. Основи застосування системи контролю версій Git. Особливості застосування систем контролю версій. Огляд технологій: GitHub, Bitbucket та GitLab. Місце Git у процесах DevSecOps.	2
Тема 6. Особливості застосування інструменту для безперервної інтеграції Jenkins. Основи розгортання системи CI/CD. Аналоги, як сервіси хмарних обчислень. Розроблення сучасного веб-застосунку у разі залучення технології CI/CD. Значність забезпечення безпеки рівня систем CI/CD.	2
Тема 7. Основи технологій захисту веб-орієнтованих систем. Особливості захисту програмних рішень. Технології Kali-Linux в завданнях тестування на вразливість, як на рівні операційної системи, так й хмарного середовища.	2
Тема 8. Основи розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps. Основи розробки SPA (Single-Page Application); застосування архітектури REST (Representational State Transfer); втілення концепції мікросервісів у сенсі залучення засобів DevSecOps. Перспективи розвитку веб-технологій та рішення завдань побудови архітектури веб-орієнтованих систем у разі неперервного циклу залучення методики DevSecOps.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Особливості сучасних мов програмування та розробки веб-орієнтованих застосунків. Аналіз безпечних практик у мовах програмування (Python, Java, JavaScript). Використання фреймворків для створення безпечних веб-додатків. Типові вразливості веб-додатків та способи їх уникнення.	4	01
Тема 2. Розгортання операційної системи Linux та Windows у якості платформи веб-сервера. Налаштування веб-сервера Apache / Nginx у Linux. Використання IIS у Windows Server. Конфігурація SSL/TLS для	4	0,1

захисту з'єднань.		
Тема 3. Особливості технологій серверної віртуалізації. Налаштування віртуальних машин у VirtualBox / VMware. Порівняння апаратної та паравіртуалізації. Практика використання Docker для контейнеризації сервісів.	4	0,1
Тема 4. Технології хмарних обчислень (Cloud Computing). Ознайомлення з платформами AWS, Azure, GCP. Створення та налаштування віртуальних серверів у хмарі. Засоби захисту та резервного копіювання у хмарних середовищах.	4	0,1
Тема 5. Основи застосування системи контролю версій Git. Основні команди Git (init, commit, push, pull, branch). Використання GitHub/GitLab для командної роботи. Захист репозиторіїв: SSH-ключі, керування доступом.	4	0,1
Тема 6. Особливості застосування інструменту для безперервної інтеграції Jenkins. Налаштування Jenkins для CI/CD. Побудова пайплайнів для автоматичного тестування та деплою. Інтеграція Jenkins із системами контролю версій та контейнерами.	4	0,1
Тема 7. Основи технологій захисту веб-орієнтованих систем. Використання WAF (Web Application Firewall). Методи захисту від SQL-ін'єкцій та XSS-атак. Аутентифікація та авторизація користувачів.	4	0,1
Тема 8. Основи розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps. Автоматизація перевірки коду на вразливості (SAST, DAST). Використання інструментів безпеки у CI/CD-процесах. Впровадження практик «Shift-left security» у розробці.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи розробки та розгортання безпечних веб-застосунків. Охоплює питання особливостей сучасних мов програмування та розробки веб-застосунків, налагодження середовища розробника в різних ОС, принципів Agile-управління. Також передбачає аналіз процесів розгортання Linux та Windows як веб-серверів, автоматизацію розгортання через Chef, Puppet, Ansible та основи безпеки серверного середовища.	0,1
Тема 1. Технології DevOps, хмарні обчислення та DevSecOps-практики. Включає теми віртуалізації (гіпервізори, контейнери), хмарних обчислень (AWS, Azure, OpenShift), системи контролю версій Git, Jenkins для CI/CD, а також основи технологій захисту веб-систем (використання Kali-Linux) та сучасні підходи DevSecOps (SPA, REST, мікросервіси, безпека CI/CD).	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи контейнеризації з Docker. Вивчення базових команд Docker, створення контейнерів, образів та забезпечення їхньої безпеки.	8
Тема 2. Kubernetes як система оркестрації контейнерів. Принципи роботи з Kubernetes, керування кластерами та механізми безпеки для контейнеризованих застосунків.	8
Тема 3. DevSecOps як розвиток DevOps. Поглиблене розуміння інтеграції безпеки в усі етапи життєвого циклу розробки програмного забезпечення.	7
Тема 4. Автоматизація інфраструктури як коду (IaC). Вивчення Terraform, Ansible та інших інструментів для безпечного керування інфраструктурою.	7
Тема 5. Безпека REST API. Методи захисту API, автентифікація, авторизація та запобігання основним атакам (наприклад, SQL Injection, XSS).	7
Тема 6. Моніторинг і логування у DevOps-середовищах. Огляд систем Prometheus, ELK (Elasticsearch, Logstash, Kibana) для контролю подій і виявлення аномалій.	7
Тема 7. Управління секретами в DevOps. Використання Vault, Kubernetes Secrets та GitHub Actions для захищеного зберігання облікових даних.	7
Тема 8. Хмарна безпека: Shared Responsibility Model. Вивчення відповідальності провайдера та клієнта у сфері хмарної безпеки (AWS, Azure, GCP).	7
Тема 9. CI/CD безпечні пайплайни. Організація пайплайнів із перевіркою безпеки коду, автоматичними тестами та статичним аналізом (SAST).	7
Тема 10. Zero Trust Architecture у DevOps. Принципи побудови безпечних систем без довіри за замовчуванням, застосування у веб-застосунках і хмарних сервісах.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «DevNet»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. DevOps Revealed 3rd edition. International DevOps Certification Academy.- 94 p. [Electronic resource]. –Access mode https://www.devops-certification.org/.
2. Розробка безпечних хмарних додатків [Електронний ресурс] / Роби Сен. IBM developerWorks, 2016. – Режим доступу : http://www.ibm.com/ developerworks/ru/library/cl-develop-secure-cloud-aware-applications/index.html.
3. Хмарні стандарти: сумісність додатків у хмарі [Електронний ресурс] / Кэйн Скарлетт. IBM developerWorks, 2016. – Режим доступу : http://www.ibm.com/ developerworks/ ru/library /cl-tools-to-ensure-cloud-application-interoperability/index.html.
4. Create REST applications with the Slim micro-framework [Electronic resource] / Vikram Vaswani. IBM developerWorks, 2012. – Access mode : http://www.ibm.com/developerworks/library/x-slim-rest/.
5. Get started with Azure [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/en-us/get-started/#explore-azure.
6. Web Application Security [Electronic resource]. – Access mode: https://www.nginx.com/resources/library/web-application-security/?utm_medium=cpc&utm_source=google&utm_campaign=emea_ne-nx_sec&utm_content=eb-textad-kywd&_bt=499136631724&_bk=devsecops&_bm=p&_bn=g&_bg=123463179768&gclid=Cj0KCQiA3rKQBhCNARIsACUEW_a0bLksBM_gH0gLf8pP0gP2z-iwk46QLUjUMDkDtq3NLHBwvANtnZYaAiEYEALw_wcB#download.
7. Tutorials Library [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/index.htm.

Додаткова література

1. Oracle Linux [Електронний ресурс]. – Режим доступу: https://www.oracle.com/linux/.
2. NIST Roadmap for Improving Critical Infrastructure Cybersecurity V [Електронний ресурс]. – Режим доступу: https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено 30.08.2025 **Завідувач кафедри** Сергій ЄВСЕЄВ

30.08.2025 **Гарант ОП** Роман КОРОЛЬОВ