Силабус освітнього компонента
Програма навчальної дисципліни

Безпека в DEVOPS

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалаврї

Тип дисципліни
Профільна, Вибіркова

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 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджженс» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua
Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування» , «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації», у студентів бакалавріата та магістратури.
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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов’язків.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов’язків.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об’єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. 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.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Розробка та аналіз алгоритмів, Фізичні основи технічних засобів розвідки, Національна безпека держави, Математичні основи криптології, 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

Теми лекційних занять

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 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.
Тема 3. Особливості технологій серверної віртуалізації.
Визначення гіпервізору та контейнерної віртуалізації. Особливості роботи із системами управління віртуальними машинами. Особливості забезпечення безпеки рівня віртуальної машини.
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.
Тема 5. Основи застосування системи контролю версій Git.

Особливості застосування систем контролю версій. Огляд технологій: GitHub, Bitbucket та GitLab. Місце Git у процесах DevSecOps.
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.
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.
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.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Особливості сучасних мов програмування та розробки веб-орієнтованих застосунків.
Тема 2. Розгортання операційної системи Linux та Windows у якості платформи веб-сервера.
Тема 3. Особливості технологій серверної віртуалізації.
Тема 4. Технології хмарних обчислень (Cloud Computing).
Тема 5. Основи застосування системи контролю версій Git.
Тема 6. Особливості застосування інструменту для безперервної інтеграції Jenkins.
Тема 7. Основи технологій захисту веб-орієнтованих систем.
Тема 8. Основи розробки сучасних веб-застосувань у сенсі залучення засобів DevSecOps.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
DevNet
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки

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

Студент 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 28.08.2024 Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024  Гарант ОП
Роман КОРОЛЬОВ