ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

DEVSECOPS І БЕЗПЕКА КОНВЕЄРІВ РОЗРОБКИ ТА ПОСТАЧАННЯ

Другого рівня вищої освіти

м. Кропивницький

1. Загальна інформація

Назва дисципліни	**DevSecOps і безпека конвеєрів розробки та постачання**
Викладач	Лектор – Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20}
E-mail:	smirnovoa@kntu.kr.ua
Консультації	*Очні консультації* відповідно до затвердженого графіку консультацій *Онлайн консультації* засобами електронної пошти, месенджерів у робочі дні

2. Анотація дисципліни

Курс **«DevSecOps і безпека конвеєрів розробки та постачання»** призначений для формування у здобувачів вищої освіти системного розуміння принципів інтеграції інформаційної безпеки в процеси розробки, тестування, розгортання та експлуатації програмного забезпечення. Курс орієнтований на вивчення сучасних підходів до побудови захищених CI/CD-конвеєрів, управління ризиками ланцюга постачання програмного забезпечення та забезпечення безпеки на всіх етапах життєвого циклу ПЗ. Вивчення дисципліни покликано наблизити студентів до реальних умов професійної діяльності, де необхідно поєднувати практики DevOps із вимогами кібербезпеки, автоматизувати контроль безпеки та оперативно реагувати на вразливості й інциденти.

3. Мета і завдання дисципліни

Метою викладання дисципліни «DevSecOps і безпека конвеєрів розробки та постачання» є формування у здобувачів вищої освіти теоретичних знань і практичних навичок впровадження підходів DevSecOps, спрямованих на забезпечення безпеки програмного забезпечення, інфраструктури та процесів постачання, а також підготовка фахівців до роботи в умовах сучасних розподілених і хмарних середовищ.

Основними завданнями вивчення дисципліни є вивчення архітектурних принципів побудови програмованих комутаторів та апаратних платформ обробки мережевого трафіку; ознайомлення з моделями програмування мережевого обладнання та підходами до реалізації логіки обробки пакетів на апаратному рівні; формування навичок аналізу та оптимізації процесів обробки трафіку з використанням спеціалізованих апаратних ресурсів; набуття практичного досвіду конфігурування та програмування мережевих пристроїв для реалізації функцій маршрутизації, фільтрації, балансування навантаження та моніторингу трафіку; розвиток здатності проєктувати ефективні мережеві рішення для датацентрів і високонавантажених мереж із урахуванням вимог до продуктивності, затримок і масштабованості.

4. Результати навчання

У результаті вивчення дисципліни здобувач вищої освіти повинен вміти:
– застосовувати принципи DevSecOps та вимоги національних і міжнародних стандартів інформаційної безпеки під час організації процесів розробки, тестування та постачання програмного забезпечення;
– аналізувати архітектуру CI/CD-конвеєрів, виявляти потенційні загрози безпеці та оцінювати ризики ланцюга постачання програмного забезпечення;
– інтегрувати засоби автоматизованого контролю безпеки (аналіз коду, перевірка залежностей, контейнерів, конфігурацій) у процеси безперервної інтеграції та розгортання;
– впроваджувати механізми керування доступом, секретами та безпечною конфігурацією інфраструктури в хмарних і датацентричних середовищах;
– здійснювати моніторинг, реагування на інциденти та оцінювання ефективності заходів безпеки в DevSecOps-середовищах.

5. Обсяг дисципліни

Ознака дисципліни	
Кількість кредитів / годин	4/120
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю	залік

6. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.
Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

7. Програма навчальної дисципліни

Тема 1. Модель загроз CI/CD-конвеєрів
Типові активи та точки атаки CI/CD.
STRIDE, attack surface конвеєра, trust boundaries.
Тема 2. Захист систем контролю версій (GitHub, GitLab, Bitbucket)
Атаки через pull/merge request.
Контроль доступу, підпис комітів, захист репозиторіїв.
Тема 3. Безпека CI/CD-агентів і runner-ів
Загрози self-hosted runner-ів.
Ізоляція, sandboxing, ephemeral runner-и.
Тема 4. Аналіз безпеки контейнерних образів у конвеєрі
Виявлення вразливостей у base-images.
Hardening Docker-образів, політики допуску.
Тема 5. Безпека Kubernetes-деплою в CI/CD
Admission Controllers і Policy as Code.
RBAC, Pod Security Standards, secrets у Kubernetes.
Тема 6. Захист Infrastructure as Code у pipeline
Вразливості Terraform, Ansible, Helm.
Автоматизований аналіз IaC до деплою.
Тема 7. Безпека програмного ланцюга постачання (Software Supply Chain)
Dependency confusion, typosquatting.
SBOM, підпис артефактів, provenance.
Тема 8. Реагування на інциденти в DevSecOps-середовищах
Компрометація pipeline.
Відновлення довіри до артефактів і середовищ..

8. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік.

Поточний контроль знань здобувачів вищої освіти здійснюється шляхом оцінювання виконання лабораторних робіт протягом семестру. При цьому враховується коректність виконання поставлених завдань, рівень обґрунтованості та аргументованості відповідей під час захисту робіт, а також дотримання визначених строків їх подання. Важливим складником оцінювання є також рівень засвоєння теоретичного матеріалу та сформованість практичних умінь і навичок.

Підсумковий контроль проводиться у формі заліку та спрямований на перевірку ступеня опанування теоретичних положень дисципліни й здатності застосовувати набуті знання під час розв'язання практичних завдань. Водночас у межах навчального процесу передбачено виконання комплексу навчальних завдань під час лекційних і лабораторних занять, а також індивідуальних робіт, що може слугувати підставою для виставлення підсумкової оцінки понад 60 балів без обов'язкового проходження залікової процедури.

9. Рекомендована література

Базова

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-cloudaware-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-toolsto-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/enus/get-started/#explore-azure.
6. Tutorials Library [Електронний ресурс]. – Режим доступу:https://www.tutorialspoint.com/index.htm.

Допоміжна

7. Oracle Linux [Електронний ресурс]. – Режим доступу: https://www.oracle.com/linux/.
8. 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-final042519.pdf
9. What is DevOps?: [Електронний ресурс]. AWS – 2020. – Режим доступу до ресурсу: https://aws.amazon.com/devops/what-is-devops

10. Peter, Naur; Brian Randell (7–11 October 1968). Software Engineering: Report of a conference sponsored by the NATO Science Committee (PDF). Garmisch, Germany: Scientific Affairs Division, NATO.
11. J.Mulder. Enterprise DevOps for Architects. Packt Publishing. BIRMINGHAM—MUMBAI, 2021. 178 c
12. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations / Gene Kim, Patrick Debois, John Willis, Jez Humble, John Allspaw / IT Revolution Press / October 6, 2016, 480p, ISBN-10 : 1942788002 ISBN-13 : 978-1942788003

Інформаційні ресурси

13. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
14. Онлайн-курси Coursera. – URL: https://www.coursera.org
15. Академія Cisco. – URL: https://www.netacad.com
16. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
17. Пошукова система. – URL:https://www.google.com/
18. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com