Силабус освітнього компонента
Програма навчальної дисципліни

Безпека серверних систем

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

ДЖЕНЮК Наталія Володимирівна

nataliia.dzheniuk@khpi.edu.ua
Доцент кафедри кібербезпеки НТУ "ХПІ" .

Кількість публікацій: понад 31, з них патентів на корисну модель 2, понад 13 наукових праць.
Фахівець з комп'ютерних мереж Cisco, кібербезпеки, інтернету речей, захисту мереж та аналітики вторгнень до мережі. Провідний лектор з дисциплін: «Безпека хмарних технологій».

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека серверних систем" є вибірковою навчальною дисципліною. Для рішення завдань бізнесу слід застосовувати не тільки ефективні та зручні IT засоби, а й приділяти велику увагу побудові контуру безпеки серверних систем. Безпека рівня серверу є необхідною складовою побудови сучасної платформи, що не є напрямком затрат для підприємства, а навпаки сприяє розвитку бізнесу та пристосування до сучасних вимог ринкової економіки.

Мета та цілі дисципліни

Дисципліна спрямована на засвоєння здобувачами теоретичних основ, формування умінь з організації безпеки серверних систем та отримання знання технологій побудови систем рівня сучасного центру обробки даних. Предметом дисципліни є інструментальні засоби та основи їх застосування у галузі адміністрування серверних систем. Об'єктом – виконання процесів налагодження та адміністрування серверних систем, а також виконання завдань їх підтримки та супроводження.

Формат занять

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

Компетентності

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Результати навчання

РН13. 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.
РН19. 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.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН23. 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.

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)

Інформаційні системи та інтернет технології, Комплексні системи захисту інформації.

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. Введення. Основні терміни та визначення. Поняття серверної системи. Загрози та ризики в серверних середовищах. Базові поняття інформаційної безпеки. Нормативно-правова база.	4
Тема 2. Особливості побудови сучасного центру обробки даних. Безпека серверних платформ Windows та Linux. Архітектура сучасного ЦОД. Мережева інфраструктура ЦОД. Безпека серверної платформи Windows. Безпека серверної платформи Linux. Моніторинг та аудит у ЦОД.	2
Тема 3. Засоби безпеки рівня серверної інфраструктури. Особливості застосування технології приватної хмари OpenStack. Засоби безпеки рівня серверу. Архітектура серверної інфраструктури. Механізми мережевої безпеки. OpenStack: архітектура та модулі. Засоби безпеки OpenStack. Безпека на рівні окремого серверу.	2
Тема 4. Технологія Kubernetes для ефективного управління контейнерами та відповідні засоби безпеки. Основи контейнеризації. Архітектура Kubernetes. Безпека контейнерів. Мережеві політики безпеки в Kubernetes. RBAC у Kubernetes. Моніторинг і аудит контейнерних середовищ.	2
Тема 5. Застосування засобів автоматизації Ansible для розгортання серверних систем. Основи конфігураційного менеджменту. Архітектура та компоненти Ansible. Автоматизація безпекових політик. Інтеграція Ansible з CI/CD. Аудит відповідності за допомогою Ansible.	2
Тема 6. Технології хмарних обчислень Red Hat OpenShift. Архітектура OpenShift. OpenShift як корпоративна Kubernetes-платформа. Безпека OpenShift. Розгортання додатків в OpenShift. Моніторинг і аудит у	2

OpenShift.	
Тема 7. Перспективи розвитку засобів безпеки у сучасному центрі обробки даних. Тренди автоматизації безпеки. Zero Trust Architecture. Квантово-стійкі алгоритми. Розвиток хмарних платформ та edge-обчислень. Еволюція стандартів та аудитів безпеки.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Розгортання веб-сервера з засобами контейнерної віртуалізації. Знайомство з засобами безпеки рівня веб-сервера та системи Docker. Студенти розгортають веб-сервер (Nginx/Apache) у контейнері Docker, налаштовують базову конфігурацію та вивчають механізми контейнерної ізоляції. Досліджуються основні параметри безпеки Docker: контроль ресурсів, робота з правами користувачів, безпечна збірка образів. Виконується базове hardening веб-сервера (SSL/TLS, заголовки безпеки, обмеження доступу).	8	0,2
Тема 2. Знайомство з засобами моніторингу серверних систем. Метою роботи є встановлення та налаштування систем моніторингу (Prometheus, Grafana або Zabbix). Студенти налаштовують збір системних метрик, створюють дашборди, аналізують навантаження серверів і контейнерів. Досліджується роль моніторингу в забезпеченні безпеки — виявлення відхилень, сповіщення, аудит подій.	8	0,2
Тема 3. Автоматизація розгортання серверних систем. Вбудова засобів безпеки у процес автоматичного розгортання кластерного рішення на базі віртуальних контейнерів. Студенти використовують Ansible для автоматичного розгортання інфраструктури контейнерного кластера (Docker Swarm / Kubernetes). Особлива увага приділяється включенню безпекових налаштувань у процес автоматизації: конфігурація фаєрволів, політики доступу, оновлення, контроль сертифікатів, мережеві політики.	8	0,2
Тема 4. Розгортання інтелектуальної системи управління кластерами контейнерів Red Hat OpenShift. У ході роботи студенти знайомляться з архітектурою OpenShift, виконують базове розгортання кластера та розміщують тестове контейнеризоване застосування. Розглядаються механізми безпеки OpenShift: Security Context Constraints, політики доступу, обмеження контейнерів, моніторинг подій та аудит. Демонструються переваги OpenShift як інтелектуальної платформи для корпоративних хмар.	8	0,2

Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Безпека серверних систем і контейнеризація. Робота спрямована на перевірку знань з основ інформаційної безпеки серверних платформ, типових загроз та механізмів захисту. Охоплює базові принципи побудови ЦОД, безпеку Windows та Linux серверів, а також основи контейнеризації Docker і способи захисту контейнерних веб-сервісів.	0,1
Тема 2. Хмарні технології, автоматизація та безпека кластерних середовищ. Контрольна оцінює розуміння студентами архітектури і безпеки хмарних платформ (OpenStack, Kubernetes, OpenShift), а також уміння застосовувати засоби автоматизації (Ansible) для створення безпечної серверної інфраструктури. Особлива увага приділяється засобам захисту кластерів і сучасним тенденціям у безпеці ЦОД.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Практики DevSecOps у сучасних IT-інфраструктурах. Інтеграція безпеки на всіх етапах розробки та експлуатації програмних систем.	8
Тема 2. Zero Trust Architecture у серверних середовищах. Принципи побудови інфраструктури без довірених зон та мінімальних прав доступу.	8
Тема 3. Використання Hardware Security Modules (HSM). Апаратні модулі для безпечного зберігання ключів та криптографічних операцій.	7
Тема 4. Системи керування журналами та SIEM-платформи. Аналіз логів, кореляція подій та виявлення інцидентів безпеки.	7
Тема 5. Форензика серверних інцидентів. Методи збору доказів, аналіз артефактів та реконструкція подій після атак.	7
Тема 6. Захист API та сервісів мікросервісної архітектури. OAuth2, JWT, rate limiting, шифрування міжсервісної взаємодії.	7
Тема 7. Ізоляція контейнерів за допомогою Seccomp, AppArmor і SELinux. Поглиблені засоби контролю доступу та обмеження привілеїв контейнерів.	7
Тема 8. Безпека мережевих сервісів у хмарних середовищах. Брандмауери, мережеві політики, сервісні сітки (Service Mesh).	7
Тема 9. Контейнерні реєстри та захист образів. Підпис образів, сканування на вразливості, довірені репозиторії.	7

Тема 10. Технології резервного копіювання в сучасних ЦОД. Підходи до backup/restore, безпека реплікацій і боротьба з ransomware.	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 «PaloAlto (SASE Fundamentals)»
https://paloaltonetworksacademy.net/course/index.php.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. [Електронний ресурс]. – Режим доступу:
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. [Електронний ресурс]. – Режим доступу:
http://kist.ntu.edu.ua/textPhD/tzi.pdf
3. David Rensin. Kubernetes. Scheduling the Future at Cloud Scale, O'Reilly Media, 2015. – 138 p. [Electronic resource]. –Access mode: https://www.openshift.com/resources/ ebooks/ kubernetes-ebook
4. Andrew Moore. OpenStack For Dummies. vScaler Limited Edition., John Wiley & Sons, Chichester, West Sussex, 2017. – 53 p. [Electronic resource]. – Access mode: https://www.vscaler.com/openstack-for-dummies/.
5. Jason Dobies, Joshua Wood. Kubernetes Operators., Red Hat, O'Reilly Media, 2020. – [Electronic resource]. –Access mode: https://www.redhat.com/cms/managed-files/cl-oreilly-kubernetes-operators-ebook-f21452-202001-en_2.pdf.

Додаткова література

6. Stefano Picozzi, Mike Hepburn, Noel O'Connor. DevOps with OpenShift, Red Hat, O'Reilly Media, 2017. – 148 p. [Electronic resource]. –Access mode: https://www.openshift.com/resources/ ebooks/devops-with-openshift/.
7. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. [[Electronic resource]. –Access mode: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. [Electronic resource]. –Access mode: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. [Electronic resource]. –Access mode: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

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** Ольга КОРОЛЬ