Силабус освітнього компонента
Програма навчальної дисципліни

Розширене адміністрування серверних сервісів

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
Науково-професійного спрямування, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

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 "Розширене адміністрування серверних сервісів" є вибірковою навчальною дисципліною. Рішення завдань адміністрування серверних систем для побудови засобів Інтернету речей (IoT, Internet of Things) обмежується не тільки автоматизацією на рівні DevOps щодо розгортання сервісів, а й поруч із цим характеризується комплексом дій щодо забезпечення моніторингу та налагодження взаємодії чималої кількості розподілених у просторі компонентів системи. Відповідна архітектура системи потребує застосування новітніх підходів щодо виконання завдань системного адміністратору з налагодження працездатності починаючи з окремого компоненту системи до комплексу IoT-рішення загалом.

Мета та цілі дисципліни

Формування у здобувача компетенцій, що грунтуються на засвоєнні знань про основні електронні компоненти і типові електронні схеми і пристрої, а також засвоєнні умінь і навичок по розробці, розрахунку і аналізу схем електронних пристроїв. Вивчення матеріалу даної дисципліни орієнтовано на широке застосування обчислювальної техніки.

Формат занять

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

Компетентності

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ7. 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.

Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН12. 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.
РН16. 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.
РН17. 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.
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.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Комплексні системи захисту інформації, Мережева та хмарна безпека, Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії), Етичний хакінг.

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. Функції ОС. Серверні операційні системи провідних виробників.	2
Тема 2, 3. Моніторинг безпеки. Файли журналів. Технології та протоколи. Моніторинг поширених протоколів HTTP та HTTPS. Протоколи електронної пошти. Списки контролю доступу. Шифрування, інкапсуляція та тунелювання. Однорангові мережі та Tor. Дані попереджень. Типи даних безпеки. Журнали кінцевих пристроїв. Журнали хостів. Системний журнал. Серверні журнали. Журнал доступу до веб-сервера Apache. Журнал доступу IIS. SIEM та колекція журналів. Мережеві журнали. Моніторинг та контроль додатків. Журнали фільтрації вмісту. Ведення журналів від пристроїв CISCO.	4
Тема 4, 5. Розуміння та використання API. Знайомство з API. Чому API так популярні. Стилі дизайну API. Архітектурні стилі API. Знайомство з REST API. REST API запити. REST API відповіді. Автентифікація в REST API. Обмеження частоти запитів API. Робота з Webhooks. Пошук та усунення проблем, пов'язаних з API викликами.	4
Тема 6. Розгортання та безпека застосунків. Розуміння варіантів розгортання за різними моделями. Середовища розгортання. Типи інфраструктури. Створення і розгортання прикладу застосунку. Безперервна інтеграція/Безперервне розгортання (CI/CD). Мережі для розробки та безпеки застосунків. Захист застосунків. Як виявити і запобігти SQL-ін'єкції. Міжсайтовий скриптинг. Еволюція систем паролів. Злам паролів.	2
Тема 7. Інфраструктура та автоматизація. Автоматизація інфраструктури за допомогою CISCO. DevOps та SRE. Основи написання скриптів автоматизації. Інструменти автоматизації. Інфраструктура як код. Автоматизація тестування. Моделювання мережі.	2
Тема 8. Платформи Cisco та розробка. Знайомство з платформами Cisco. Cisco SDK. Вивчення можливостей програмованості мережі та моделей пристроїв. Керування мережею Cisco. Керування обчисленнями Cisco. Платформи співпраці Cisco. Платформи безпеки Cisco.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Розгортання веб-серверу у середовищі віртуальної машини. Знайомство із засобами безпеки рівня веб-сервера. Ознайомлення з процесом створення, налаштування та запуску веб-сервера у віртуальному середовищі (наприклад,	8	0,2

VirtualBox, VMware).		
Тема 2. Установка та налагодження веб-сервера на базі брокера повідомлень за протоколом MQTT або ін. Вивчення принципів роботи брокерів повідомлень та їх інтеграції з веб-серверами.	8	0,2
Тема 3. Тестування роботи розподіленої системи реєстрації та обробки даних за технологією Інтернету речей (IoT). Перевірка працездатності системи збору та обробки даних із сенсорів у розподіленій мережі.	8	0,2
Тема 4. Розгортання інтелектуальної системи рівня розумного будинку. Застосування платформи IFTTT. Ознайомлення з принципами побудови автоматизованих систем управління на базі IoT.	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. Адміністрування веб-серверів та забезпечення їх безпеки. Розглядаються принципи встановлення, налаштування та оптимізації роботи веб-серверів (Apache, Nginx), а також методи їх захисту від типових кібератак. Аналізуються засоби шифрування з'єднань (SSL/TLS), управління доступом і журнали подій для моніторингу безпеки.	0,1
Тема 2. Серверні сервіси в інфраструктурі Інтернету речей (IoT). Вивчаються особливості адміністрування серверних компонентів, що забезпечують взаємодію IoT-пристроїв, зокрема брокерів повідомлень (MQTT, AMQP), баз даних і хмарних сервісів. Оцінюється надійність, продуктивність і безпечність розподілених систем.	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. Архітектура клієнт-серверних систем. Основні принципи побудови серверної інфраструктури, взаємодія клієнтських і серверних компонентів.	8
Тема 2. Віртуалізація серверів та контейнеризація. Ознайомлення з технологіями VMware, Hyper-V, Docker, Kubernetes; порівняння підходів і переваг.	8
Тема 3. Автоматизація розгортання серверних сервісів.	7

Практичне застосування Ansible, Puppet, Chef для управління конфігураціями та оновленнями.	
Тема 4. Моніторинг та управління продуктивністю серверів. Інструменти Nagios, Zabbix, Prometheus, Grafana для збору метрик і виявлення аномалій.	7
Тема 5. Резервне копіювання та відновлення серверних систем. Стратегії створення бекапів, використання rsync, Bacula, Veeam, а також планування Disaster Recovery.	7
Тема 6. Управління користувачами та правами доступу. Контроль безпеки через ACL, групові політики, PAM, SELinux, AppArmor.	7
Тема 7. Адміністрування баз даних на серверному рівні. Оптимізація, безпека та резервування БД MySQL, PostgreSQL, MongoDB.	7
Тема 8. Захист серверної інфраструктури від кібератак. Практичні аспекти роботи з міжмережевими екранами, IDS/IPS-системами, honeypots.	7
Тема 9. Інтеграція серверів з хмарними платформами. Використання AWS, Azure, Google Cloud для масштабування серверних сервісів.	7
Тема 10. Контейнерна оркестрація та мікросервісна архітектура. Впровадження CI/CD-процесів, управління контейнерами та сервісами у DevOps-середовищі.	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, CCNA3»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Johansson L., Vinka. E. The optimal RabbitMQ guide. From Beginner to Advanced - An introduction to RabbitMQ and CloudAMQP. - 84codes AB, 2020. – 138 p. . [Electronic resource]. –Access mode: https://www.cloudamqp.com/rabbitmq_book_success.html.
2. Maarten van SteenAndrew S. Tanenbaum. Distributed Systems. Third edition., Maarten van Steen, 2018. – p. [Electronic resource]. – Access mode: https://www.distributed-systems.net/index.php/contact/.
3. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. URL:
http://kist.ntu.edu.ua/textPhD/tzi.pdf.

4. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с. URL: http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf
5. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с. URL: https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover

Додаткова література

6. Налаштування середовища безперервного розгортання за допомогою Jenkins [Електронний ресурс] / Лв, Чжао Чжо, Янь Чже, Чень Сяо Лун. IBM developerWorks, 2015. - Режим доступу: https://www.ibm.com/developerworks/ru/library/d-continuous-delivery-framework-jenkins/.
7. 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/.
8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. 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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. 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.
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** Станіслав МІЛЕВСЬКИЙ