Силабус освітнього компонента
Програма навчальної дисципліни

Основи планування та адміністрування служб доступу до інформаційних ресурсів

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

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-наукової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

Детальніше про викладача на сайті кафедри

МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua

Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Ігрове та системно-динамічне моделювання кіберконфліктів», «Computer networks», у студентів бакалавріата та магістратури.

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 "Основи планування та адміністрування служб доступу до інформаційних ресурсів" є вибірковою навчальною дисципліною. Дисципліна спрямована на придбання навичок з проектування та створення інформаційного ресурсу для малого підприємства, а також комплексних практичних навичок щодо планування, адміністрування та забезпечення безпеки служб доступу до інформаційних ресурсів.

Мета та цілі дисципліни

Формування у студентів теоретичних знань з основ планування та адміністрування служб доступу до інформаційних ресурсів, до яких у більшості відносяться сучасні системи керування вмістом, за допомогою яких реалізовуються веб-ресурси та сервіси, а також формування практичних навичок із побудови та адміністрування відповідних серверних систем.

Формат занять

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

Компетентності

КЗК–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗК–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

СК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

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.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
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.
ПРН-18. 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)

Архітектура та захист сучасних операційних систем, Комп'ютерні мережі, Безпека в інформаційно-комунікаційних системах.

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 CMS (Content Management System). Класифікація CMS: open-source та комерційні. Порівняння популярних CMS (WordPress, Joomla, Drupal). Архітектурні особливості CMS. Критерії вибору CMS для проєктів різного масштабу.	2
Тема 2. Ймовірність і статистика у ШІ. Теорія прийняття рішень на основі ймовірностей. Основи ймовірнісних розподілів. Умовні ймовірності, Байєсівські мережі, закони великих чисел. Теорія Байєса та її застосування у ШІ. Прогнозування на основі ймовірнісних моделей.	2
Тема 3. Математичний аналіз та його застосування у ШІ. Похідні, градієнти, інтеграли. Градієнтний спуск: основи та модифікації (стохастичний, міні-батч). Методи моделювання. Інструменти для симуляції. Прикладні задачі моделювання.	2
Тема 4. Теорія графів та алгоритми на графах. Базові поняття графів: вершини, ребра, ступені. Алгоритми пошуку на графах та їх використання у штучному інтелекті.	2
Тема 5. Чисельні методи у задачах ШІ. Основи чисельної лінійної алгебри. Методи для розв'язування лінійних систем та найменших квадратів.	2
Тема 6. Математичні основи оптимізації. Задачі оптимізації у машинному навчанні. Градієнтний спуск та методи прискорення оптимізації (метод Ньютона, моментум).	2
Тема 7. Методи регуляризації у машинному навчанні. L1 та L2 регуляризація. Проблема перенавчання та боротьба з ним за допомогою регуляризації.	2
Тема 8. Основи теорії інформації та ентропії. Визначення інформації та ентропії. Крос-ентропія, дивергенція Кульбака-Лейблера та їх використання в алгоритмах ШІ.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1 Вивчення мережевих засобів доступу до інформаційних систем. Основні протоколи мережевого доступу (HTTP, HTTPS, FTP, SSH). Налаштування клієнтських засобів доступу. Використання засобів моніторингу та аналізу трафіку.	2	0,1
Тема 2. Розгортання віртуальної машини на базі Linux. Вибір програмного забезпечення для віртуалізації (VirtualBox, VMware). Створення віртуальної машини та налаштування ресурсів. Встановлення та базове адміністрування Linux.	2	0,1
Тема 3. Розгортання веб-серверу та засобів управління базами даних. Встановлення та налаштування Apache/Nginx. Встановлення MySQL/MariaDB. Конфігурація взаємодії веб-сервера з базою даних.	2	0,1
Тема 4. Розгортання WordPress. Завантаження та встановлення WordPress. Налаштування підключення до бази даних. Базові параметри сайту та перші записи.	2	0,1
Тема 5 Застосування засобів LDAP. Основи побудови каталогів LDAP. Встановлення та налаштування OpenLDAP. Тестування доступу користувачів через LDAP.	2	0,1
Тема 6 Взаємодія та обмін інформацією у системі на базі WordPress. Управління користувачами та ролями. Організація комунікацій між користувачами. Інтеграція плагінів для обміну даними.	2	0,1
Тема 7 Програмування доступу до API. Основні принципи REST API. Використання інструментів для тестування API (Postman). Розробка простих скриптів для доступу до API.	2	0,1
Тема 8 Засоби безпеки сайту на базі WordPress. Налаштування прав доступу та ролей. Використання плагінів безпеки. Захист від атак типу SQL Injection та XSS.	2	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{m} a_i$=0,8

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Організація доступу до інформаційних ресурсів. Мережеві протоколи та засоби доступу. Віртуалізація як засіб адміністрування доступу. Використання LDAP у системах ідентифікації та автентифікації.	0,1
Тема 2. Адміністрування та безпека веб-ресурсів. Розгортання веб-сервера і баз даних. Інсталяція та налаштування WordPress. Засоби безпеки та захисту від кіберзагроз у CMS.	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. Хмарні технології у забезпеченні доступу до інформаційних ресурсів. Переваги та ризики використання хмарних рішень у адмініструванні.	8
Тема 2. Механізми автентифікації та авторизації. Методи контролю доступу: парольні системи, багатофакторна автентифікація, токени.	8
Тема 3. Засоби шифрування даних у мережевих службах. Використання SSL/TLS, VPN та інструментів для захисту переданих даних.	7
Тема 4. Контейнеризація сервісів (Docker, Kubernetes). Використання контейнерів для ізоляції та адміністрування служб доступу.	7
Тема 5. Системи моніторингу та логування. Застосування Prometheus, Grafana, ELK-стека для відстеження роботи сервісів.	7
Тема 6. Захист від DDoS-атак. Методи запобігання та нейтралізації масових атак на веб-ресурси.	7
Тема 7. Політики управління користувачами в ОС Linux. Налаштування прав доступу, груп користувачів та контроль активності.	7
Тема 8. Засоби резервного копіювання та відновлення даних. Підходи до збереження даних і забезпечення безперервності роботи систем.	7
Тема 9. Міжмережеві екрани та системи виявлення вторгнень (IDS/IPS). Принципи побудови та використання для захисту доступу.	7
Тема 10. Перспективи розвитку CMS та їх інтеграція з іншими сервісами. Використання API, мікросервісної архітектури та інновацій у системах управління контентом.	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 «Network Defence»
https://www.netacad.com/catalogs/learn?category=course.

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.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf
2. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ: навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.
https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/e0d0e0cc-d807-4b6f-af0b-54aad9bcc9bf/content
3. Microservices vs. Service-Oriented Architecture. Mark Richards. / O'Reilly Media. All., 2016., 57 p. [Electronic resource]. –Access mode: https://www.oreilly.com/radar/microservices-vs-service-oriented-architecture/.
4. UNIX and Linux System Administration Handbook URL:
https://mog.dog/files/SP2019/2017%20Nemeth%20Evi%20etal%20-%20UNIX%20and%20Linux%20System%20Administration%20Handbook%5B5thED%5D_Rell.pdf.

Додаткова література

1. WordPress User Manual for Beginners URL: https://www.epecorp.com/assets/wordpress_user_manual.pdf.
2. WordPress PDF Manual URL: https://wp-tutoring.com/wordpress-pdf-manual-now-available/.
3. 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
4. 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
5. 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:

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

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