Силабус освітнього компонента
Програма навчальної дисципліни

Архітектура та захист сучасних операційних систем

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
4

Мова викладання
Українська, англійська

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

Загальна інформація

Анотація

Навчальна дисципліна "Архітектура та захист сучасних операційних систем" є обов'язковою навчальною дисципліною. Дисципліна спрямована на освоєння принципів використання системного програмного забезпечення, операційної системи персонального комп'ютера (сервера) для підтримання його в робочому стані; знання основних понять теорії побудови операційних систем; запобігання шляхів несанкціонованого доступу до даних операційної системи; вживання заходів протидії проникненню шкідливого програмного забезпечення до середовища операційної системи.

Мета та цілі дисципліни

Засвоєння теоретичних основ побудови, принципів проектування, конфігурування й застосування різних сучасних операційних систем, які забезпечують організацію обчислювальних процесів у корпоративних інформаційних системах економічного, управлінського, виробничого, наукового й іншого призначення, а також надання практичних навичок щодо захисту даних в сучасних операційних систем.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

Результати навчання

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 180 год. (6 кредитів ECTS): лекції – 32 год., лабораторні роботи – 48 год., самостійна робота – 100 год.

Передумови вивчення дисципліни (пререквізити)

Фізика, Математичні основи криптології.

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. Вступ. Архітектура та ресурси сучасних операційних систем. Вступ до сучасних операційних систем.	4
Тема 2. Планування та керування процесами та потоками. Процеси та потоки. Планування процесів. Управління процесами. Механізми межпроцесорної взаємодії.	4
Тема 3. Керування оперативною пам'яттю. Керування пам'яттю.	4
Тема 4. Комплексна система захисту даних операційної системи. Основи захисту сучасних ОС.	4
Тема 5. Автентифікація та управління доступом до операційної системи. Автентифікація в СОС.	4

Тема 6. Безпека облікового запису. Розуміння SUID/SGID. Аудит файлів SUID/SGID. Налаштування sudo. Розуміння su. Встановлення паролів користувачів. Застарілі паролі користувачів. Доступ до безпеки мережі. Процеси доступу до файлів. Встановлення обмежень для користувачів. Перегляд поточних користувачів. Перегляд історії входу.	4
Тема 7. Налаштування безпеки хоста. Розуміння xinetd. Розуміння одиниць systemd.socket. Налаштування обгорток TCP. Заборона доступу користувачам. Розуміння init. Скрипти ініціалізації.	4
Тема 8. Захист даних за допомогою шифрування. Розуміння OpenSSH. Налаштування клієнта OpenSSH. Аутентифікація та ключі SSH. Клієнтські утиліти SSH. Тунелювання SSH. Розуміння GnuPG.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Розгортання ОС Windows на віртуальній машині. Ознайомлення з поняттям віртуалізації. Встановлення VirtualBox/VMware. Налаштування параметрів віртуальної машини. Інсталяція ОС Windows у віртуальному середовищі. Оптимізація продуктивності віртуальної машини.	3	1
Тема 2. Дискреційний механізм розмежування доступу до файлових об'єктів. Поняття дискреційного доступу. Робота з правами доступу до файлів і каталогів. Налаштування дозволів (Read, Write, Execute). Використання ACL (Access Control List). Аналіз вразливостей при неправильному налаштуванні доступу.	3	1
Тема 3. Вивчення процесів, потоків, дескрипторів та реєстру Windows. Поняття процесів та потоків. Використання інструментів для моніторингу процесів (Process Explorer). Дескриптори в ОС Windows та їх роль. Основи роботи з системним реєстром. Аналіз впливу процесів на безпеку ОС.	3	1
Тема 4. Використання Windows PowerShell. Основи роботи з PowerShell. Виконання базових команд. Створення скриптів PowerShell. Автоматизація адміністративних задач. PowerShell як інструмент атаки та захисту.	3	1
Тема 5. Диспетчер завдань Windows. Огляд інтерфейсу диспетчера завдань. Виявлення ресурсомістких процесів. Аналіз запущених служб і програм. Використання диспетчера для діагностики проблем. Практичні кейси виявлення шкідливих процесів.	3	1
Тема 6. Моніторинг системних ресурсів у Windows та управління ними. Використання Performance Monitor. Відстеження процесора, пам'яті, дисків та мережі. Збір логів і побудова графіків. Виявлення аномалій у роботі системи. Практичне використання моніторингу для кіберзахисту.	3	1

Тема 7. Процедура відновлення або обнулення забутого пароля. Огляд способів скидання пароля. Використання стандартних інструментів Windows. Використання LiveCD/Recovery Disk. Потенційні ризики та методи захисту від несанкціонованого відновлення. Практична демонстрація атаки «Offline Password Reset».	3	1
Тема 8. Аналіз кадрів Ethernet за допомогою програми Wireshark. Ознайомлення з Wireshark. Захоплення мережевого трафіку. Аналіз протоколів Ethernet, TCP, UDP, HTTP. Виявлення підозрілої активності. Практичні методи приховування та захисту даних у мережі.	3	1
Тема 9. Розгортання системи для тестування на проникнення Kali Linux. Інсталяція Kali Linux на віртуальній машині. Огляд основних інструментів Kali. Виконання базових тестів на проникнення. Порівняння з іншими дистрибутивами Linux. Практика безпечного тестування.	3	1
Тема 10. Адміністрування безпеки. Принципи адміністрування безпеки ОС. Налаштування політик безпеки. Контроль облікових записів користувачів. Використання Group Policy. Практика управління безпекою корпоративної мережі.	3	1
Тема 11. Extended Internet Super-Server (xinetd). Призначення та функції xinetd. Встановлення і налаштування. Контроль доступу через xinetd. Журнали подій і моніторинг. Практичні приклади застосування.	3	1
Тема 12. Configuring TCP Wrappers. Призначення TCP Wrappers. Конфігураційні файли /etc/hosts.allow та /etc/hosts.deny. Налаштування доступу до сервісів. Приклади практичної конфігурації. Інтеграція TCP Wrappers із системами IDS/IPS.	3	1
Тема 13. TCP Wrappers (поглиблене вивчення). Поглиблені принципи роботи TCP Wrappers. Використання з різними сервісами Linux. Виявлення та блокування підозрілих підключень. Логи та звітність. Обмеження технології.	3	1
Тема 14. Налаштування адреси управління комутатором. Основи налаштування комутаторів. Консольний доступ до комутатора. Призначення IP-адреси для управління. Тестування підключення через Telnet/SSH. Методи захисту доступу до комутатора.	3	1
Тема 15. GPG (GNU Privacy Guard). Основи криптографії з відкритим ключем. Встановлення та налаштування GPG. Генерація ключів. Шифрування та підпис повідомлень. Використання GPG для захисту електронної пошти.	3	1
Тема 16. Використання віртуалізації та контейнеризації для підвищення безпеки ОС. Основи контейнеризації (Docker). Порівняння віртуальних машин і контейнерів. Запуск ізольованих додатків у	3	1

контейнерах. Практика забезпечення безпеки контейнерів. Приклади використання в корпоративних системах.		
Загальна кількість годин	**48**	$\sum_{i=1}^{n} a_i = 16$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Архітектура сучасних операційних систем і моделі захисту. Порівняння монолітної, мікроядерної та гібридної архітектур ОС. Механізми керування процесами та потоками. Системні виклики і їхній вплив на безпеку. Моделі безпеки (Bell-LaPadula, Biba, Clark-Wilson) у контексті ОС.	1
Тема 2. Механізми автентифікації та контролю доступу в ОС. Методи автентифікації користувачів (парольні, біометричні, токени). Дискреційні, мандатні та рольові моделі контролю доступу. Використання ACL та SELinux/AppArmor. Типові вразливості та атаки на механізми автентифікації.	1,5
Тема 3. Захист мережевої взаємодії в операційних системах. Протоколи безпеки (SSL/TLS, IPsec). Засоби моніторингу та аналізу мережевих з'єднань. Використання TCP Wrappers і xinetd. Практика протидії атакам «Man-in-the-Middle» та «Sniffing».	1,5
Загалом	$\sum_{i=1}^{m} b_i=4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Історія та еволюція операційних систем. Поява перших ОС. Монолітні, мікроядерні та гібридні ОС. Вплив архітектури на безпеку та стабільність системи.	10
Тема 2. Сучасні ОС для серверів та робочих станцій. Windows Server та Linux-дистрибутиви для корпоративного використання. Особливості безпеки та адміністрування.	10
Тема 3. Керування процесами та потоками. Механізми планування процесів. Синхронізація потоків та захист від гонок. Права доступу до процесів.	10
Тема 4. Файлові системи та механізми контролю доступу. NTFS, ext4, ZFS: структура та безпека. ACL та права користувачів. Шифрування даних на рівні файлової системи.	10
Тема 5. Методи автентифікації та авторизації. Паролі, ключі, сертифікати, біометрія. Двофакторна автентифікація. Принцип найменших привілеїв.	10
Тема 6. Моніторинг та аудит безпеки. Логи системи та подій безпеки. Інструменти моніторингу (SIEM). Виявлення аномалій та інцидентів.	10

Тема 7. Мережеві протоколи та безпека. TCP/IP, UDP, ICMP: загрози та захист. VPN, SSH, TLS/SSL. Аналіз трафіку та фільтрація пакетів.	10
Тема 8. Віртуалізація та контейнери. Hypervisor та типи віртуалізації. Безпека віртуальних машин та контейнерів Docker. Ізоляція процесів та ресурсів.	10
Тема 9. Тестування безпеки ОС. Пентестинг та етичний хакинг. Виявлення вразливостей та патч-менеджмент. Використання Kali Linux та Metasploit для навчальних цілей.	10
Тема 10. Сучасні тенденції в захисті ОС. Zero Trust та принципи кібергігієни. Використання штучного інтелекту для захисту. Хмарні системи та безпека віддаленого доступу.	10
Загальна кількість годин	**100**

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 «Operating System Basics»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Волосюк Ю .В. Комп'ютерні мережі: курс лекцій / Ю. В. Волосюк. – Миколаїв : МНАУ, 2019. – 203 с.
https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni_merezhi_kurs_lektsii.pdf
2. Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211 p.,2011.
https://books.google.com.ua/books/about/Security_for_Microsoft_Windows_System_Ad.html?id=6kykvSXhkv4C&redir_esc=y
3. Stallings, William. Operating systems: internals and design principles / William Stallings. – 7 th ed. Prentice Hall, New Jersey, 2012, p.769. ISBN-13:978-0-13-230998-1.
4. Kusswurm Daniel. Modern X86 Assembly Language Programming/ Daniel Kusswurm. - Apress, 2019. — 604 p.
https://www.academia.edu/36380133/Daniel_Kusswurm_Modern_X86_Assembly_Language_Programming_32_bit_64_bit_SSE_and_AVX_Apress_2014_
5. Russell S. R., Taylor B. W. Operations management : Creating value along the supply chain. 7 ed. N.-Y. : John Wiley & Sons, Inc., 2010. 832 p.
http://jtelen.free.fr/0MARINE%20bouquins/%5BRoberta_S._Russell,_Bernard_W._Taylor%5D_Operations(Bookos.org).pdf
6. Haseman Chris. Android Essentials / Chris Haseman. – Apress, 2008. – 116 p.
https://books.google.com.ua/books/about/Android_Essentials.html?id=ASmO8r7i93sC&redir_esc=y
7. J.Spealman, K.Hudson, M.Graft, Windows Server 2003: Active Directory Infrastructure. Microsoft Press, pp. 1–8–1–9, 2003.

8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf

Додаткова література

9. William Stallings. Operating Systems: Internals and Design Principles, 9th Edition. – Pearson, 2018. ISBN-10: 0-13-467095-7 | ISBN-13: 978-0-13- 467095-9.
https://books.google.com.ua/books/about/Operating_Systems.html?id=u5M5nQAACAAJ&redir_esc=y
10. Шеховцов В. А. Операційні системи / В. А. Шеховцов – К.: Вид.гр. BHV, 2005. – 576 с.
https://f.eruditor.link/file/2315933/

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
0,6	0,4		

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** Сергій ЄВСЕЄВ