Силабус освітнього компонента
Програма навчальної дисципліни

Адміністрування UNIX-подібних систем

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320

Спеціалізація
-

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
7

Мова викладання
Українська

Викладачі, розробники

ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua
Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua
Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми "Національна безпека у сфері кіберзахисту" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: «Мережне програмування», «Розробка та аналіз алгоритмів», «Технології програмування» , «Інструментальні засоби програмування», «Веб безпека», «Основи технічного захисту інформації», у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Адміністрування UNIX-подібних систем" є вибірковою навчальною дисципліною. В рамках даного курсу даються базові знання з завдань, методів вирішення і інструментам системного адміністрування UNIX. Розглядається широке коло повсякденних завдань системного адміністратора: від управління призначеними для користувача бюджетами та до установки, настройки, настроїти загальні компонент системи і прикладного програмного забезпечення.

Мета та цілі дисципліни

Навчання студентів для адміністрування UNIX-подібних систем, показати відмінності і подібні риси широкого спектра UNIX систем. В ході курсу ілюструються особливості різних UNIX-подібних систем: Linux, FreeBSD, Solaris.

Формат занять

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

Компетентності

ЗК1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ЗК8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.
СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
РН2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
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.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
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.
РН15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної 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.
РН18. 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)

Основи програмування. Технології програмування.

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. Початкове завантаження і зупинка системи. Початкове завантаження і зупинка системи. Облікові записи користувачів.	2
Тема 2. Параметри завантаження ядра системи. Налагодження параметрів завантаження ядра системи.	2
Тема 3. Конфігурація ядра системи. Налагодження параметрів ядра системи.	2
Тема 4. Термінальний доступ в систему. Налагодження параметрів термінального доступу до системи.	2
Тема 5. Управління сховищами даних. Налагодження параметрів сховищ даних.	2
Тема 6. Адміністрування системних служб. Налагодження параметрів системних служб.	2
Тема 7. Використання менеджера пакетів. Налагодження параметрів менеджеру пакетів.	2
Тема 8. Параметри безпеки системи. Налагодження параметрів безпеки системи.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Початкове завантаження і зупинка системи. Ознайомлення з процесом старту та завершення роботи UNIX-подібної системи, порядок виконання init-процесів, Runlevel та	4	0,1

systemd.		
Тема 2. Параметри завантаження ядра системи. Вивчення конфігурації завантажувача (GRUB/LILO), параметрів ядра, які впливають на запуск системи та апаратне обладнання.	4	0,1
Тема 3. Конфігурація ядра системи. Практика налаштування ядра UNIX-подібної системи, підключення/відключення модулів та оптимізація під потреби системи.	4	0,1
Тема 4. Термінальний доступ в систему. Використання терміналів і оболонок (shell), віддалений доступ через SSH, налаштування прав користувачів.	4	0,1
Тема 5. Управління сховищами даних. Робота з файловими системами, монтування/розмонтування дисків, розділи, RAID, контроль використання простору.	4	0,1
Тема 6. Адміністрування системних служб. Налаштування та контроль системних демонів, робота з systemd, запуск, зупинка та автоматичне завантаження служб.	4	0,1
Тема 7. Використання менеджера пакетів. Встановлення, оновлення та видалення пакетів у UNIX-подібних системах за допомогою apt, yum, pacman та інших менеджерів.	4	0,1
Тема 8. Налагодження параметрів безпеки системи. Основи забезпечення безпеки системи, налаштування прав доступу, файрволів, SELinux/AppArmor та політик користувачів.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

За наявності

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Початкове завантаження і зупинка системи. Облікові записи користувачів. Перевірка знань студентів щодо процесу старту та завершення роботи UNIX-подібної системи, порядку виконання init-процесів та управління обліковими записами користувачів. Включає завдання на аналіз Runlevel/systemd, створення та налаштування користувачів, груп та прав доступу.	0,1
Тема 2. Параметри завантаження та конфігурації ядра, термінальний доступ, управління сховищами та системними службами. Перевірка знань студентів щодо налаштування параметрів завантаження ядра, конфігурації ядра, термінального доступу, управління сховищами та системними службами. Включає практичні завдання з редагування конфігураційних файлів, налаштування служб через systemd, монтування/розмонтування файлових систем та керування правами доступу.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та екзамену.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Історія та різновиди UNIX-подібних систем. Ознайомлення з походженням UNIX, основними дистрибутивами Linux, BSD та їх особливостями.	7
Тема 2. Файлова система UNIX. Структура файлової системи, права доступу, типи файлів та робота з каталогами.	7
Тема 3. Командний рядок та оболонки (Shell). Основи роботи в командному рядку, популярні оболонки (bash, zsh), написання простих скриптів.	7
Тема 4. Процеси та керування ними. Моніторинг і управління процесами, сигнали, пріоритети та планувальники.	7
Тема 5. Планування завдань (cron, at). Автоматизація виконання завдань за розкладом, налаштування cron-джобів та одноразових завдань.	7
Тема 6. Менеджери пакетів та оновлення системи. Встановлення, оновлення та видалення програмного забезпечення за допомогою apt, yum, pacman та інших.	7
Тема 7. Мережеві налаштування UNIX-систем. Основи налаштування мережі, перегляд стану інтерфейсів, базові команди ping, netstat, ifconfig/ip.	7
Тема 8. Моніторинг системи та журналювання. Використання системних журналів (syslog/journalctl), моніторинг ресурсів та навантаження.	7
Тема 9. Резервне копіювання та відновлення даних. Методи резервного копіювання, утиліти tar, rsync, налаштування автоматичних бекапів.	8
Тема 10. Основи безпеки UNIX-систем. Керування правами доступу, користувачами та групами, налаштування файрволу, SELinux/AppArmor.	8
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 «Linux Essentials»
https://www.netacad.com/catalogs/learn?category=course

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations Paperback – Illustrated, October 6, 2016.
https://training.epam.ua/ua/blog/564.
2. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation (Addison-Wesley Signature Series (Fowler)) 1st Edition.
https://proweb.md/ftp/carti/Continuous-Delivery-Jez%20Humble-David-Farley.pdf.
3. Nicole Forsgrenjez, Humblegene Kim: Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations.
https://books.google.com.ua/books/about/Accelerate.html?id=85XHAQAACAAJ&redir_esc=y.
4. Ansible: Up and Running, 2nd Edition by Lorin Hochstein, Rene Moser Released August 2017 Publisher(s): O'Reilly Media, Inc.
https://digtvbg.com/files/LINUX/Meijer%20B.%20Ansible.%20Up%20and%20Running...3ed%202022.pdf.
5. Javascript Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/javascript/index.htm
6. UNIX / LINUX Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/unix/index.htm.
7. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.

Додаткова література

1. Tutorials Library [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/index.htm

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** Роман КОРОЛЬОВ