



Силабус освітнього компонента

Програма навчальної дисципліни



Адміністрування UNIX-подібних систем

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалаврї

Тип дисципліни

Профільна, Вибіркова

Семестр

7

Мова викладання

Українська

Викладачі, розробники



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 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](#)



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 " 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-1. 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.

КЗ-2. 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.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність спілкуватися державною мовою як усно, так і письмово.

КЗ-5. Здатність спілкуватися іноземною мовою.

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

КЗ-8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.

ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-1. 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.

ПРН-2. 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.

ПРН-3. 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.

ПРН-4. Вільно спілкуватися державною мовою.

ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційною безпекою.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

ПРН-11. 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.

ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною 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.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. 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 – 32 год., лабораторні роботи – 16 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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Початкове завантаження і зупинка системи.

Початкове завантаження і зупинка системи. Облікові записи користувачів.

Тема 2. Параметри завантаження ядра системи.

Налагодження параметрів завантаження ядра системи.

Тема 3. Конфігурація ядра системи.

Налагодження параметрів ядра системи.

Тема 4. Термінальний доступ в систему.

Налагодження параметрів термінального доступу до системи.

Тема 5. Управління сховищами даних.

Налагодження параметрів сховищ даних.

Тема 6. Адміністрування системних служб.

Налагодження параметрів системних служб.

Тема 7. Використання менеджера пакетів.

Налагодження параметрів менеджера пакетів.

Тема 8. Параметри безпеки системи.

Налагодження параметрів безпеки системи.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Початкове завантаження і зупинка системи.

Тема 2. Параметри завантаження ядра системи.

Тема 3. Конфігурація ядра системи.

Тема 4. Термінальний доступ в систему.

Тема 5. Управління сховищами даних.

Тема 6. Адміністрування системних служб.

Тема 7. Використання менеджера пакетів.

Тема 8. Налагодження параметрів безпеки системи.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://sur.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження

професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:

Linux Essentials

<https://www.netacad.com/catalogs/learn?category=course>.

Література та навчальні матеріали

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 Forsgren, Jez Humble: 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. Євсєєв, А.М.

Ткачов, В.О. Алексєєв, 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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

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

Студент 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

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Роман КОРОЛЬОВ