



## СИЛАБУС ДИСЦИПЛІНИ «СИСТЕМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ» (вибіркова)

Ступінь вищої освіти – Бакалавр  
Спеціальність 125 – КІБЕРБЕЗПЕКА  
Освітня програма «Кібербезпека»  
Рік навчання 4, семестр 7  
Форма навчання денна  
Кількість кредитів ЄКТС 5  
Мова викладання українська

Лектор курсу



Коваленко Олексій Єпифанович,  
професор кафедри комп'ютерних систем,  
мереж та кібербезпеки, доктор технічних наук  
([портфоліо](#))

Контактна інформація  
лектора (e-mail)

Кафедра комп'ютерних систем, мереж та кібербезпеки,  
корпус. 15, к. 207, тел. 5278724  
e-mail [O.Kovalenko@nubip.edu.ua](mailto:O.Kovalenko@nubip.edu.ua)  
ЕНК <https://elearn.nubip.edu.ua/course/view.php?id=1929>

Сторінка курсу в eLearn

### ОПИС ДИСЦИПЛІНИ

**Завдання** вибіркової навчальної дисципліни «Системне програмне забезпечення» – вивчення основ організації та використання системного програмного забезпечення у комп'ютерних системах та мережах, дослідження проблем конфігурування, аналізу, управління, забезпечення ефективного використання системного програмного забезпечення в організаціях і на підприємствах різних напрямків діяльності та різних форм власності.

**Місце і роль дисципліни** в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в області комп'ютерної інженерії.

#### Компетентності ОП:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

#### Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ЗК 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

#### Спеціальні (фахові) компетентності:

СК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК 13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

#### **Програмні результати навчання (ПРН) ОП:**

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

### **СТРУКТУРА КУРСУ**

<b>Тема</b>	<b>Години (лекції/ лабораторні)</b>	<b>Результати навчання</b>	<b>Завдання</b>	<b>Оцінювання</b>
<b>Модуль 1</b>				
Види та організація системного програмного забезпечення (СПЗ).	4/4	Знати організацію СПЗ та вміти застосовувати теоретичні знання та практичні навички для розв'язування задач вибору та аналізу СПЗ при розробці комп'ютерних систем для агропромислового комплексу країни.	Опитування у вигляді есе з основних теоретичних питань.	5
Архітектура СПЗ операційних середовищ (ОС) комп'ютерних систем (КС).	4/4	Вміти здійснювати опис архітектурних компонентів ОС та знати способи їх застосування.	Захист лабораторної роботи. Виконання самостійної роботи (Неформальна on-line освіта на основі МВОК).	5
Файлові систем	4/4	Вміти користуватись СПЗ для	Захист лабораторної	

КС.		обслуговування файлових систем та аналізувати вплив конфігурації СПЗ на їх параметри.	роботи.	<b>5</b>
Надійність файлових систем.	<b>4/4</b>	Вміти використовувати засоби управління файловими системами та аналізувати їх стан.	Захист лабораторної роботи.	<b>5</b>
<b>Модульний контроль</b>			Модульний тест в ЕНК	<b>10</b>

<b>Модуль 2</b>				
Диспетчеризація і синхронізація в ОС.	<b>2/2</b>	Знати моделі станів ОС та вміти аналізувати потоки і процеси в КС.	Захист лабораторної роботи.	<b>5</b>
Засоби конфігурування СПЗ. Реєстр ресурсів КС.	<b>4/4</b>	Знати структуру реєстру ОС та вміти аналізувати його параметри.	Захист лабораторної роботи.	<b>5</b>
Системні сервіси та їх організація.	<b>4/4</b>	Знати організацію системних сервісів, вміти їх створювати та здійснювати керування	Захист лабораторної роботи.	<b>5</b>
Засоби системного адміністрування.	<b>4/4</b>	Знати призначення, можливості організацію системних оболонок адміністрування СПЗ. Вміти їх використовувати для управління та аналізу операційного середовища КС.	Захист лабораторної роботи.  (Неформальна on-line освіта на основі МВОК).	<b>5</b>  <b>10</b>
<b>Модульний контроль</b>			Модульний тест в ЕНК.	<b>10</b>
<b>Всього за семестр</b>				<b>70</b>
<b>Екзамен</b>				<b>30</b>
<b>Всього за курс</b>				<b>100</b>

### **ПОЛІТИКА ОЦІНЮВАННЯ**

<b><i>Політика щодо контрольних термінів та перескладання:</i></b>	Контрольні терміни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрадження).
<b><i>Політика щодо академічної доброчесності:</i></b>	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв).
<b><i>Політика щодо відвідування:</i></b>	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

### **ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ**

<b>Рейтинг здобувача вищої освіти, бали</b>	<b>Оцінка національна за результати складання екзаменів заліків</b>	
	<b>Екзаменів</b>	<b>Заліків</b>
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано