МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативного освітнього компонента
ОПЕРАЦІЙНІ СИСТЕМИ
Підготовки першого (бакалаврського) рівня вищої освіти
Спеціальності 125 Кібербезпека та захист інформації
Освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2024

Силабус нормативного освітнього компонента «Операційні системи» підготовки бакалаврів, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації

Розробник:
Булатецький Віталій Вікторович, кандидат фізико-математичних наук, доцент, доцент кафедри комп'ютерних наук та кібербезпеки

Погоджено

Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</td><td>Характеристика освітнього компонента</td></tr>
<tr><td>Нормативна</td></tr>
<tr><td>Денна форма навчання</td><td rowspan="7">Галузь знань
12 Інформаційні технології,
спеціальність
125 Кібербезпека та захист інформації,
освітньо-професійна програма
Кібербезпека та захист інформації
освітній рівень бакалавр.</td><td>Рік підготовки 2</td></tr>
<tr><td rowspan="4">Кількість
Годин/кредитів
120/4</td><td>Семестр 3</td></tr>
<tr><td>Лекції 30 год.</td></tr>
<tr><td>Лабораторні 42 год.</td></tr>
<tr><td>Самостійна робота 40 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: екзамен.</td></tr>
<tr><td colspan="3">Мова навчання – Українська</td></tr>
</table>

ІІ Інформація про викладача

ПІП: Булатецький Віталій Вікторович;
Науковий ступінь: кандидат фізико математичних наук;
Вчене звання: доцент;
Посада: доцент кафедри комп'ютерних наук та кібербезпеки;
Контактна інформація: Bulatetsky.Vitaly@vnu.edu.ua
Дні занять: http://94.130.69.82/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація курсу. Силабус освітнього компонента складено відповідно до освітньо-професійної програми підготовки бакалаврів Кібербезпека та захист інформації. Освітній компонент «Операційні системи» належить до переліку освітніх компонент циклу професійної підготовки, забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, вмінь та навичок роботи з різними операційними системами.

Предметом вивчення освітнього компонента є операційні системи, методи та засоби адміністрування операційних системам та їх захисту.

2. Мета вивчення освітнього компонента. Формування у слухачів знань, вмінь та навичок роботи з різними операційними системами та з методами та засобами, пов'язаними із захистом в операційних системах. Основними завданнями вивчення освітнього компонента «Операційні системи» є ознайомлення слухачів з еволюцією та класифікацією операційних систем, вивчення їх функціоналу, засобів захисту та підтримки цілісності.

3. Перелік компетентностей випускника

Загальні компетентності

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 8. 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.

Спеціальні (фахові, предметні) компетентності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних систем згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

Програмні результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

РН 4. 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.

РН 5. 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.

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту зметою оперативного відновлення функціонування інформаційної системи.

4. Структура освітнього компонента

Освітня компонента складається з таких змістових модулів:
Змістовий модуль 1. Принципи побудови та класифікація операційних систем.
Змістовий модуль 2. Адміністрування операційних систем.
Змістовий модуль 3. Методи та засоби захисту операційних систем.

Назви змістових модулів і тем	Кількість годин					Форма контролю / бали
	Усього	у тому числі				
		Лек.	Лаб.	Сам. роб.	Конс.	
Змістовий модуль 1. Принципи побудови та класифікація операційних систем						Кр /30 балів
1. Поняття операційної системи. Еволюція та класифікація операційних систем.	7	2	4		1	Лр/3 бали
2. Принцип модульності. Принцип функціональної вибірковості. Принцип генерування ОС. Принцип функціональної надмірності. Принцип віртуалізації. Принцип незалежності програм від зовнішніх пристроїв. Принцип сумісності. Принцип відкритої і нарощуваної ОС. Принцип мобільності (переносимості). Принцип забезпечення безпеки обчислень	7	4		2	1	
3. Операційні мережеві системи. Структурне представлення ОС. Однорангові та дворангові мережеві ОС. Типи мережевих ОС.	4	2		2		
4. Мікроядерні ОС. Мікроядерна архітектура. Переваги і недоліки мікроядерної архітектури. Ядро і допоміжні модулі ОС. Багатошарова структура ОС.	7	2	2	2	1	Лр/2 бали
5. Ієрархія даних. Файли. Файлові системи. Типи розподілу пам'яті. Загальна модель ФС. Права доступу, багатокористувацький режим та кешування диску.	11	2	4	4	1	Лр/3 бали
6. Особливості областей використання багатозадачних ОС. Вимоги до ОС реального часу.	4	2		2		
7. Огляд реальних актуальних ОС.	10	2	6	2		Лр/6 балів
Разом за змістовим модулем 1	**50**	**16**	**16**	**14**	**4**	**44 балів**
Змістовий модуль 2. Адміністрування операційних систем.						Кр /10 балів
1. Основні задачі адміністрування.	7	2		4	1	
2. Моніторинг роботи операційної системи.	10	2	4	4		Лр/4 бали
3. Методи та засоби адміністрування.	23	2	10	10	1	Лр/10 балів
Разом за змістовим модулем 2	**40**	**6**	**14**	**18**	**2**	**24 бали**
Змістовий модуль 3. Методи та засоби захисту операційних систем.						Кр /20 балів
1. Основні загрози безпеці інформації в операційних системах.	5	2		2	1	
2. Вимоги до захищеності інформації і критерії оцінювання систем щодо безпеки оброблюваної інформації	4	2		2		
3. Механізми і засоби захисту, які впроваджуються в операційних системах	13	2	8	2	1	Лр/8 балів
4. Відмовостійкість операційних систем	8	2	4	2		Лр/4 бали

Разом за змістовим модулем 3	**30**	**8**	**12**	**8**	**2**	**32 бали**
Всього годин/Балів	**120**	**30**	**42**	**40**	**8**	**100 балів**

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт. Оформлення результатів лабораторних робіт	**16**
2	Опрацювання лекційного матеріалу	**16**
3	Систематизація здобутих знань перед екзаменом. Робота з літературними джерелами.	**8**
	Разом	**40**

IV. Політика оцінювання

Політика щодо академічної доброчесності. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі здобувачами.

Політика щодо перескладання. 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).

Політика щодо оскарження оцінювання. Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми навчання відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати відповідними документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту. За об'єктивних причин навчання може відбуватись в он-лайн формі за погодженням з керівником курсу та деканом факультету.

Додаткові бали. Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освітим буде нараховано додаткові бали за активність на заняттях, за вчасно здані роботи, за відсутність пропусків без поважних причин. Згідно Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки здобувач освіти може додатково отримати до 20 % максимального поточного балу.

Визнання результатів навчання, отриманих у формальній, неформальній освіті. Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність здобувачів на території України чи поза її межами, для здобувачів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Підсумковий контроль

Форма контролю – семестровий екзамен. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль (нараховується за якісне виконання лабораторних робіт) та підсумковий модульний контроль (нараховується за виконання модульних контрольних робіт та модульних тестових робіт). Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи, модульні тестові завдання і складає максимум 60 балів.

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому випадку здобувач складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів, при цьому бали за підсумковий модульний контроль анульовуються.

Екзамен проходить в усній формі. Оцінка за семестр у випадку складання іспиту є сумою балів поточного контролю та балів, отриманих під час іспиту.

Питання, які виносяться на екзамен

1. Поняття операційної системи. Еволюція та класифікація операційних систем.
2. Принцип модульності. Принцип функціональної вибірковості. Принцип генерування ОС. Принцип функціональної надмірності. Принцип віртуалізації. Принцип незалежності програм від зовнішніх пристроїв. Принцип сумісності. Принцип відкритої і нарощуваної ОС. Принцип мобільності (переносимості). Принцип забезпечення безпеки обчислень
3. Операційні мережеві системи. Структурне представлення ОС. Однорангові та дворангові мережеві ОС. Типи мережевих ОС.
4. Мікроядерні ОС. Мікроядерна архітектура. Переваги і недоліки мікроядерної архітектури. Ядро і допоміжні модулі ОС. Багатошарова структура ОС.
5. Ієрархія даних. Файли. Файлові системи. Типи розподілу пам’яті. Загальна модель ФС. Права доступу, багатокористувацький режим та кешування диску.
6. Особливості областей використання багатозадачних ОС. Вимоги до ОС реального часу.
7. Огляд реальних актуальних ОС.
8. Основні задачі адміністрування.
9. Моніторинг роботи операційної системи.
10. Методи та засоби адміністрування.
11. Основні загрози безпеці інформації в операційних системах.

12. Вимоги до захищеності інформації і критерії оцінювання систем щодо безпеки оброблюваної інформації.
13. Механізми і засоби захисту, які впроваджуються в операційних системах.
14. Відмовостійкість операційних систем.

Екзамен проходить у вигляді виконання комплексних завдань різного типу (тестові завдання, розв'язування задач, усне опитування).

1. Тестові завдання, 20 запитань по 1 балу, всього 20 балів. (тестові завдання охоплюють всі теми змістових модулів: питання, які виносяться на екзамен).

2. Практичне завдання 1 типу, всього 20 балів. (завдання готуються на основі завдань до лабораторних робіт та охоплюють всі теми лабораторних робіт).

3. Одне теоретичне запитання 20 балів за повну відповідь (питання, які виносяться на екзамен).

Типи практичних завдання:

Встановити Linux Ubuntu mini x32 18.04 з базовим набором компонентів. Встановити ssh (openssh-server), net-tools, mc, nano, vim. Доєднатись віддалено через SSH (через Putty або Powershell). Встановити GUI на вибір та інтернет-браузер і продемонструвати його роботу. Створити трьох користувачів з різними привілеями.

V. Шкала оцінювання

Шкала оцінювання (національна та ECTS)

Оцінка в балах за всі види навчальної діяльності	**Оцінка**
90 – 100	Відмінно
82 – 89	Дуже добре
75 81	Добре
67 74	Задовільно
60 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси

1. Powershell Tutorial. *Online Tutorials Library*. URL: https://www.tutorialspoint.com/powershell/index.htm (дата звернення: 04.09.2024).
2. Windows PowerShell Scripting Tutorial for Beginners. *Netwrix Blog | Insights for Cybersecurity and IT Pros*. URL: https://blog.netwrix.com/powershell-scripting-tutorial/ (дата звернення: 04.09.2024).
3. Batch-file eBook. *Learn programming languages with books and examples*. URL: https://riptutorial.com/ebook/batch-file (дата звернення: 04.09.2024).
4. An A-Z Index of Windows CMD commands - SS64.com. *SS64 Command line reference*. URL: https://ss64.com/nt/ (дата звернення: 04.09.2024).
5. Булатецький В. В., Булатецька Л. В., Гришанович Т. О. Аналіз файлових об'єктів операційної системи Windows 10 для очищення й оптимізації простору системного розділу. *Кібербезпека: освіта, наука, техніка.* 2022. Т. 3, № 15. С. 71–84. DOI: https://doi.org/10.28925/2663-4023.2022.15.7184.

6. Research methods and tools for cleaning the system partition of Windows operating systems / A. P. Stupin, V. V. Bulatetskyi, L. V. Bulatetska, T. O. Hryshanovych, Yu. S. Pavlenko. *Computer Science & Software Engineering (CS&SE@SW 2021)* : Proceedings of the 4th Workshop for Young Scientists, Kryvyi Rih, 18 December 2021. 2022. P. 135–145. URL: http://ceur-ws.org/Vol-3077/paper17.pdf.
7. Operation system features and cloud services for lecturer work / L. V. Bulatetska, V. V. Bulatetskyi, T. O. Hryshanovych, Yu. S. Pavlenko, T. I. Cheprasova, A. V. Pikilnyak. *Cloud Technologies in Education (CTE 2020)* : Proceedings of the 8th Workshop, Kryvyi Rih, 18 December 2020. 2021. P. 148–151. URL: http://ceur-ws.org/Vol-2879/paper14.pdf.