

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

СУЧАСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ХМАРНІ ТЕХНОЛОГІЇ

підготовки бакалавра

спеціальності 125 Кібербезпека

освітньо-професійної програми Інформаційна безпека

Луцьк – 2022

Силабус навчальної дисципліни «Сучасне програмне забезпечення та хмарні технології» підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, за освітньою програмою Інформаційна безпека

Розробник: Глинчук Л. Я., доцент кафедри комп'ютерних наук та кібербезпеки, кандидат фізико-математичних наук.

Погоджено

Гарант освітньо-професійної програми:



Глинчук Л.Я.

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

протокол № 2 від 29 вересня 2022 р.

Завідувач кафедри:



Гришанович Т. О.

І. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітньо-професійна /освітньо-наукова/освітньо-творча програма, освітній рівень	Характеристика освітнього компонента
Денна форма навчання	<i>12 Інформаційні технології</i> <i>125 Кібербезпека</i> <i>Інформаційна безпека</i> <i>Бакалавр</i>	Нормативний
Кількість годин/кредитів 120/4		Рік навчання: I
		Семестр: 1
		Лекції: 28 год.
		Лабораторні роботи: 36 год.
ІНДЗ: немає		Самостійна робота: 48 год.
		Консультації: 8 год.
		Форма контролю: залік
Мова навчання		Українська

ІІ. Інформація про викладача

ППП Глинчук Людмила Ярославівна

Науковий ступінь кандидат фізико-математичних наук

Вчене звання -

Посада доцент кафедри комп'ютерних наук та кібербезпеки

Контактна інформація тел.: 095 890 42 46,

e-mail: Hlynchuk.Ludmila@vnu.edu.ua

Дні занять <http://194.44.187.20/cgi-bin/timetable.cgi?n=700>

ІІІ. Опис дисципліни

1. Анотація курсу. В дисципліні розглядаються загальні відомості про програмне забезпечення, класифікація та види сучасного програмного забезпечення, програмне забезпечення прикладного та службового рівнів рекомендованого для організації робочого місця студентів комп'ютерних спеціальностей, види ліцензій ПЗ, відкрите ПЗ, законодавство у сфері ПЗ. Розглядаються базові відомості про виникнення, розвиток та використання хмарних технологій, моделі надання хмарних послуг, переваги хмарних технологій; архітектура (типології розгортання хмарних ресурсів – приватні, публічні, гібридні) і пропозиції від провідних компаній надання хмарних послуг, досвід використання хмарних технологій за кордоном; безпека у хмарних сервісах, загрози для безпеки у хмарі та пропозиції захисту від них.

В дисципліні передбачено огляд сучасних рішень лідерів ринку хмарних обчислень – Microsoft, Google та інших.

Для розвитку практичних навичок пропонується виконання завдань у різних хмарних середовищах.

2. Пререквізити. Дисципліна читається на I курсі у I семестрі, тому необхідне вміння та знання основ роботи в мережі Інтернет та офісними програмами.

Постреквізити. Здобуті знання можуть бути використані під час вивчення професійних навчальних дисциплін, при написанні курсової роботи та спільних проектів.

3. Мета і завдання навчальної дисципліни.

Мета: ознайомлення студентів з основними поняттями сучасного програмного забезпечення та хмарних технологій, набуття здатностей (компетенцій) ефективно реалізовувати теоретичні знання у повсякденному житті та у своїй практичній та професійній діяльності.

Завдання: ознайомлення з видами сучасного програмного забезпечення та хмарних сервісів і особливостями їх використання, ознайомлення з основними провайдерами хмарних послуг і їх технічною базою, оволодіння навичками використання сучасного програмного забезпечення та хмарних технологій для роботи з інформацією, її зберігання та захисту, у навчанні, для спільної роботи над проектами.

4. Результати навчання (Компетентності) відповідно до освітньо-професійної програми

Загальні компетентності (ЗК):

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності (ФК):

ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.

ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки

ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою.

Програмні результати навчання

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН5. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

5. Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основні поняття сучасного програмного забезпечення та хмарних технологій						
Тема 1. Класифікація програмного забезпечення	7	2	2	3		IPC/2
Тема 2. Безкоштовне та ліцензійне ПЗ. Види ліцензій	8	2	2	3	1	IPC/2
Тема 3. Оновлення ПЗ та сумісність. Тестування на сумісність	7	2	2	3		IPC/2
Тема 4. Моделі надання хмарних послуг. Переваги хмарних технологій	7	2	2	3		IPC/2
Тема 5. Архітектура і пропозиції від провідних компаній надання хмарних послуг, досвід використання хмарних технологій за кордоном	9	2	2	4	1	IPC/2
Тема 6. Безпека у хмарних сервісах	10	2	4	4	1	IPC/4
Тема 7. Загрози для безпеки у хмарі та пропозиції захисту від них	9	2	2	4	1	IPC/2
Разом за модулем 1	57	14	16	24	4	16
Змістовий модуль 2. Практика використання хмарних середовищ						
Тема 8. Використання хмарного сервісу Google Apps: сховище Google Drive, обліковий запис, робота з таблицями та документами	8	2	4	2		IPC/4
Тема 9. Використання хмарного сервісу Google Apps: створення сайтів на Google Sites	8	2	2	4		IPC/2
Тема 10. Використання хмарного сервісу Google Apps: створення форми засобами Google Forms (переваги використання хмарних сервісів	9	2	2	4	1	IPC/2

для створення Інтернет-опитувань)						
Тема 11. Використання хмарного середовища OneDrive сервіс Microsoft, зокрема Forms: створення опитувань (переваги використання хмарних сервісів для створення Інтернет-опитувань)	9	2	2	4	1	IPC/2
Тема 12. Хмаро орієнтований пакет програм Microsoft Office 365 та робота в ньому	13	2	6	4	1	IPC/8
Тема 13. Аналіз захищеності у хмарних середовищах Google Apps та Microsoft Office 365	8	2	2	4		IPC/3
Тема 14. Хмарна технологія для створення динамічних презентацій Prezi	8	2	2	2	1	IPC/3
Разом за модулем 2	63	14	20	24	4	24
Види підсумкових робіт						Бал
Контрольна робота № 1 (Тести + індивідуальне завдання)						15
Контрольна робота № 2 (Тести або усне опитування)						25
Індивідуальна робота студента (IPC)						20
Всього годин/ Балів	120	28	36	48	8	100

6. Завдання для самостійного опрацювання

№	Тема
1.	Інсталювати та деінсталювати різне ПЗ: системне, прикладне, інструментальне, порівняти процес інсталяції, деінсталяції, затребуваність пам'яті та ресурсів.
2.	Визначити особливості ПЗ різних ліцензій.
3.	Опрацювати українське законодавство у сфері захисту програмного забезпечення
4.	Опрацювати стратегії захисту у хмарних середовищах
5.	Опрацювати стандарти захисту у сфері хмарних технологій
6.	Здобути практичні навички у інших хмарних середовищах, що пропонують створення інтерактивних публікацій, стрічок часу, створення графічних елементів, схем, відео та іншого контенту
7.	Опрацювати хмарні антивіруси, визначити їх особливості
8.	Опрацювання теоретичного матеріалу та підготовка лабораторних робіт
9.	Підготовка до заліку

IV. Політика оцінювання

Політика викладача щодо студента

Освоєння дисципліни передбачає обов'язкове відвідування лекцій і лабораторних занять, а також самостійну роботу.

Поведінка в аудиторії.

Усі учасники освітнього процесу мають дотримуватися етичних норм.

Студент зобов'язаний старанно та сумлінно навчатися протягом усього періоду отримання освіти. Водночас він повинен підтримувати інших у прагненні поглиблювати знання та виконувати свої обов'язки.

Від викладача вимагається доброзичливе, серйозне і тактовне ставлення до здобувачів вищої освіти.

Студент, який спізнився з неповажних причин, вважається таким, що пропустив заняття з виставленням відмітки пропуску у журнал, але при цьому має право бути присутнім на занятті. За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття.

Політика щодо академічної доброчесності

Академічна доброчесність.

Дотримання академічної доброчесності студентами передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;
- посилення на джерела інформації у разі використання відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання;
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика щодо дедлайнів та перескладання

Усі передбачені завдання, мають бути виконані у встановлений термін. За несвоєчасно виконані завдання буде накладено штраф – будуть відніматися бали за відповідну лабораторну роботу. Виключенням можуть бути завдання, які не вдалося зробити з поважних причин, в такому випадку студент може доробити вказані завдання у вказаний термін.

V. Підсумковий контроль

Підсумковий контроль з даної дисципліни передбачено у вигляді заліку.

Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе поточний контроль, який нараховується за виконання лабораторних робіт, індивідуальних робіт, контрольних робіт, тестових робіт до лекційних матеріалів курсу. Максимальна кількість балів, яку може отримати студент під час поточного оцінювання за семестр – 100 балів. Якщо за результатами семестру студент отримав не менше 60 балів і погоджується

із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому випадку студент складає залік; максимальна кількість балів, яку можна отримати – 100 балів.

Порядок проведення заліку – залік відбувається або у вигляді тестування (складається база питань за весь семестр) або у вигляді практичного завдання та усної відповіді на теоретичні питання.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти, де формою контролю є залік

Оцінка в балах	Лінгвістична оцінка
90–100	Зараховано
82–89	
75–81	
67–74	
60–66	
1–59	Незараховано (необхідне перескладання)

VI. Рекомендована література та інтернет-ресурси

Основна література

1. Вакалюк Т.А. Хмарні технології в освіті. Навчально-методичний посібник для студентів фізико-математичного факультету. – Житомир: вид-во ЖДУ, 2016. – 72 с.
2. Красний С.І. Хмарні технології: методичні рекомендації для самостійної роботи слухачів курсів підвищення кваліфікації /С.І. Красний. – Біла Церква:– БІНПО УМО, 2017. – 83 с.
3. Войтович Н.В., Найдьонова А.В. Використання хмарних технологій Google та сервісів web 2.0 в освітньому процесі. Методичні рекомендації. – Дніпро: ДПТНЗ «Дніпровський центр ПТОТС», 2017 – 113 с.
4. Введение в облачные вычисления/ И. Л. Клементьев, В. А. Устинов - М : Национальный Открытый Университет "ИНТУИТ", 2016. – 311 с.
5. Жилін В.А, Панасенко Д.П., Класифікація сучасного програмного забезпечення службового та прикладного рівнів, рекомендованого для організації робочого місця студентів комп'ютерних спеціальностей. Системи обробки інформації, 2014, випуск 5 (121). ISSN 1681-7710. – с. 177-182.
6. Аулов І.Ф., Дослідження моделі закріплення ключових систем хмари та пропозиції захисту від них. Восточно-Европейский журнал передовых технологий 5/2 (77) 2015, ISSN 1729-3774, DOI: 10.15587/1729-4061.2015.50912, - С.13

Додаткова література (інтернет-джерела)

1. Загрози для безпеки у хмарі: відповіді на часті запитання. [Електронний ресурс]. – Режим доступу до ресурсу: <https://www.de-novo.biz/blog/zagrozi-dlya-bezpeki-u-hmari-vidpovidi-na-chasti-zapitannya-17>
2. Різновиди ПЗ. Презентація. [Електронний ресурс]. – Режим доступу до ресурсу: <https://svitppt.com.ua/informatika/riznovidi-programnogo-zabezpechennya-ponyattya-operaciynoi-sistemi-ta-.html>
3. Класифікація ПЗ. [Електронний ресурс]. – Режим доступу до ресурсу: https://stud.com.ua/53323/informatika/programne_zabezpechennya
4. Лучшие бесплатные программы на каждый день. [Електронний ресурс]. – Режим доступу до ресурсу: <https://remontka.pro/best-free-software/>
5. Дослідження: 80% всього ПЗ в Україні – неліцензійне. [Електронний ресурс]. – Режим доступу до ресурсу: <https://www.epravda.com.ua/news/2018/09/19/640732/>
6. Реєстр виробників та розповсюджувачів ПЗ. [Електронний ресурс]. – Режим доступу до ресурсу: <https://data.gov.ua/dataset/ce13eef2-80f0-4ff2-9b31-40722e429059/resource/b5539268-9bde-462f-881c-bfab0e2297d>
7. Використання комп'ютерних програм: «что такое хорошо, что такое плохо» [Електронний ресурс]. – Режим доступу до ресурсу: <https://i.factor.ua/ukr/journals/nibu/2012/july/issue-56/article-61158.html>
8. Список відкритого ПЗ. [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F

VII. Питання до заліку

1. Прикладне програмне забезпечення. Види та приклади.
2. Системне програмне забезпечення. Види та приклади.
3. Інструментальне програмне забезпечення. Види та приклади.
4. Класифікація програмного забезпечення для підприємств, за ступенем тиражованості, за призначенням, за видами, за способом розповсюдження і т.д.
5. Класифікаційні групи програмного забезпечення (Управління електронними базами даних, "BackUp" – класифікаційна група програм, що забезпечують резервне копіювання і т.д.)
6. Ліцензія на ПЗ та її види.
7. Безкоштовне (вільне) ПЗ. Де брати та приклади.
8. Види безоплатного ПЗ. Приклади для декількох видів.
9. Ліцензійне ПЗ і контрафакт: як відрізнити?
10. Що таке ТОП ПЗ? Як визначити та на що слід звернути увагу?
11. Що таке оновлення ПЗ? Для чого це потрібно робити для ПК?
12. Чому варто оновлювати програмне забезпечення на пристроях Android? Перерахувати та охарактеризувати усі причини.
13. Динамічне оновлення програмного забезпечення(ДОПЗ). Існуючі ДОПЗ системи.
14. Сумісність програмного забезпечення, сумісність апаратного забезпечення.
15. Зворотня сумісність в програмному та апаратному забезпечення. Переваги та недоліки.
16. Тестування сумісності ПЗ. Види тестувань на сумісність.

17. Моделі надання хмарних послуг: модель SaaS. Популярні продукти SaaS.
18. Моделі надання хмарних послуг: модель PaaS. Популярні продукти PaaS.
19. Моделі надання хмарних послуг: модель EaaS. Популярні продукти EaaS.
20. Моделі надання хмарних послуг: модель Daas. Популярні продукти Daas.
21. Моделі надання хмарних послуг: інші моделі (IaaS, Waas, BaaS).
22. Моделі надання хмарних послуг: інші моделі (HaaS, DBaaS, WaaS).
23. Переваги хмарних технологій.
24. Категорія хмар за формою власності: приватна хмара (Private Cloud).
25. Категорія хмар за формою власності: громадська (Community Cloud).
26. Категорія хмар за формою власності: публічна хмара (Public Cloud).
27. Категорія хмар за формою власності: гібридна хмара (Hybri Cloud).
28. Досвід використання хмарних технологій закордоном.
29. Проблеми пов'язані з безпекою та ризики використання хмар.
30. Безпека хмарних сервісів від особливості діяльності.
31. Управління безпекою у хмарі: стримуюче та профілактичне управління.
32. Управління безпекою у хмарі: детективне та коригуюче управління.
33. Атаки на хмари і рішення щодо їх усунення.
34. Стандарт безпеки ISO/IEC 27018 та головні принципи хмар згідно його.
35. Можливі загрози хмарних обчислень та методи (інструменти) забезпечення безпеки (на прикладі).
36. Google Drive (Диск): створення аккаунту, інтерфейс стартової сторінки.
37. Google Drive (Диск): функції кнопок, міток, закладка «Налаштування».
38. Google Drive (Диск): панель інструментів «Дії», доступи до папки та до документу.
39. Google Drive (Диск): способи створення гугл-документу, гугл-таблиці, можливості дій з папкою та з файлом (меню правої кнопки миші).
40. Основні переваги та недоліки використання сервісу Google Sites.
41. Створення сайту за допомогою сервісу Google Sites.
42. Особливості Google Forms (Форми).
43. Google Forms (Форми): інтерфейс та панелі інструментів.
44. Google Forms (Форми): процес створення тестів та налаштування відповідей.
45. Використання хмарного середовища OneDrive сервіс Microsoft: Forms (створення опитувань) процес створення опитувань.
46. Використання хмарного середовища OneDrive сервіс Microsoft: Forms (створення опитувань) усі необхідні налаштування.
47. Хмаро орієнтований пакет програм Microsoft Office 365 та робота в ньому: особливості та робота у Microsoft Teams.
48. Хмаро орієнтований пакет програм Microsoft Office 365 та робота в ньому: особливості та робота Microsoft Stream.
49. Користуючись хмарним середовищем Microsoft Office 365: детально розглянути роботу у Word, Excel, визначити особливості.
50. Користуючись хмарним середовищем Microsoft Office 365: детально розглянути роботу у Outlook, PowerPoint, визначити особливості.
51. Процес створення презентації засобом SharePoint від Microsoft Office 365.
52. Використання хмарного середовища OneDrive сервіс Microsoft: створення документів та папок, надання доступів.
53. Налаштування та рекомендації, які допомагають захистити аккаунт Google.
54. Програма додаткового захисту аккаунту Google.
55. OneDrive: додатковий захист найважливіших файлів у Сейфі та нові сховища.

56. Захисний комплекс Microsoft. Комплексний захист хмарного середовища.
57. Технології безпеки Microsoft Azure.
58. Інструкція зі створення презентацій у системі Prezi.
59. Меню «Insert» («Вставити») у системі Prezi.
60. Додавання зверстаних слайдів. Додавання/зміна фонової музики у системі Prezi.
61. Імпорт файлів та презентацій. Український шрифт у системі Prezi.
62. Збереження, завантаження, відображення та видалення презентації в мережі.