

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ


Кафедра економічної кібернетики


«ЗАТВЕРДЖУЮ»
декан факультету інформаційних
технологій
Глазунова О.Г.
2022 р.

Протокол №10 від 19 травня 2022 р.

"СХВАЛЕНО"

на засіданні кафедри економічної кібернетики
Протокол №10 від 06 травня 2022 р.
Завідувач кафедри


Дмитро ЖЕРЛІЦІН

"РОЗГЛЯНУТО"

Гарант ОПІ «Цифрова економіка»


Дмитро ЖЕРЛІЦІН

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Інформаційна безпека економічних систем»

Галузь знань **05** «Соціальні та поведінкові науки»
Спеціальність **051** «Економіка»
Освітньо-професійна програма «Цифрова економіка»

Розробник:

доцент кафедри економічної кібернетики, к.е.н., доцент Негрей М.В.

Київ – 2022 р.

1. Опис навчальної дисципліни

Інформаційна безпека економічних систем

Галузь знань, напрям підготовки, спеціальність, ступень вищої освіти	
Освітній ступінь	<i>Бакалавр</i>
Галузь знань	05 Соціальні та поведінкові науки;
Спеціальність	051 Економіка;
Освітня програма	Цифрова економіка
Характеристика навчальної дисципліни	
Вид	Обов'язкова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістовних модулів	2
Курсовий проект (робота) (за наявності)	Не передбачено
Форма контролю	Екзамен
Показники навчальної дисципліни	
Форма навчання	<i>Денна</i>
Рік підготовки	<i>3</i>
Семестр	<i>6</i>
Лекційні заняття	<i>30</i>
Практичні, семінарські заняття	
Лабораторні заняття	<i>30</i>
Самостійна робота студента	<i>60</i>
Індивідуальні завдання	
Кількість тижневих аудиторних годин для денної форми навчання	<i>4 год.</i>

2. Мета, завдання та компетентності навчальної дисципліни

Мета вивчення курсу – систематизація знань студентів в галузі інформаційної безпеки організацій різних форм власності та вивчення прикладних особливостей застосування методів та засобів захисту інформації.

Завдання вивчення курсу

- оволодіння основними термінами та формуванні системи знань щодо інформаційної безпеки економічних систем;
- вивчення автоматизованих економічних інформаційних систем, їх складових елементів, особливостей інформаційних і розрахункових задач у складі програмного забезпечення;
- оволодінні основами проектування елементів програмного забезпечення інформаційних систем;
- вивченні та опрацюванні практичних особливостей розробки, впровадження та використання інформаційних і розрахункових задач та їх комплексів.

Після вивчення курсу студент повинен **вміти** визначати:

- основні поняття інформаційної безпеки та автоматизованих економічних інформаційних систем;
- загрози інформаційної безпеки та причини її порушення;
- складові системи захисту інформації;
- основи та складові такого специфічного засобу захисту інформації, як шифрування;
- особливості захисту інформації від комп'ютерних вірусів;
- характеристики структури та життєвого циклу комп'ютерних вірусів, правила захисту від них;
- значення термінів "інформаційна безпека", "автоматизована інформаційна система", "інформаційна технологія";
- класифікацію автоматизованих інформаційних систем та їх особливості;
- структуру програмного забезпечення електронної обчислювальної машини;
- складові загального та спеціального програмного забезпечення та їх функції;

- класифікацію інформаційних і розрахункових задач залежно від характеру переробки інформації, призначення та рівня застосування;
- основні вимоги до розробки спеціального програмного забезпечення;
- принципи розробки та використання спеціального програмного забезпечення;
- етапи процесу створення інформаційних і розрахункових задач;
- порядок впровадження та використання інформаційних і розрахункових задач та їх комплексів.

Навчальна дисципліна забезпечує формування ряду загальних компетентностей:

ЗК9. Здатність до адаптації та дій в новій ситуації.

ЗК10. Здатність бути критичним і самокритичним.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

СК17. Здатність обґрунтовувати управлінські рішення щодо забезпечення інформаційної та цифрової безпеки бізнесу, захисту економічної інформації і персональних даних.

СК20. Здатність до роботи з сучасними системами та інструментами захисту цілісності та доступності економічної інформації.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 6. Використовувати професійну аргументацію для донесення інформації, ідей, проблем та способів їх вирішення до фахівців і нефахівців у сфері економічної діяльності.

ПРН 15. Демонструвати базові навички креативного та критичного мислення у дослідженнях та професійному спілкуванні.

ПРН17. Виконувати міждисциплінарний аналіз соціально-економічних явищ і проблем в однієї або декількох професійних сферах з врахуванням ризиків та можливих соціально-економічних наслідків.

ПРН 22. Демонструвати гнучкість та адаптивність у нових ситуаціях, у роботі із новими об'єктами, та у невизначених умовах.

ПРН 25. Знати основні принципи, напрями і механізми цифрової економіки та вміти пояснювати її об'єктивну необхідність цифрової трансформації суспільних відносин.

ПРН 29. Демонструвати здатність застосовувати засоби і методи інформаційної та цифрової безпеки для захисту бізнес-інформації і персональних даних.

ПРН 30. Показувати навички проектувати, моделювати та створювати бази даних та знань з використанням структурованої мови запитів SQL та будувати на їх основі інформаційні системи.

3. Програма навчальної дисципліни

Змістовний модуль 1. Теоретичні основи інформаційної безпеки економічних систем.

Тема 1. Основні аспекти інформаційної безпеки економічних систем.

Уточнення сутності ключових категорій: "інформаційна безпека", "політика безпеки", "інформаційна загроза", "інформаційна війна", "інформаційний вплив", "інформаційна зброя", Визначення критеріїв захищеної системи обробки інформації та постановка задач, вирішення яких дозволить створити дану систему. Формалізація класифікації загроз інформаційної системи та характеристика причини їх виникнення.

Тема 2. Поняття інформаційних загроз та їх види.

Загальна характеристика основних причин порушення інформаційної безпеки. Визначення загальних підходів щодо помилок в системах захисту, що призводять до їх вразливості. Поняття "загрози безпеки інформації", причини їх виникнення, їх види та особливості прояву. Характеристика засобів і способів захисту інформації.

Тема 3. Принципи побудови системи інформаційної безпеки.

Державне регулювання інформаційної безпеки. Підходи, принципи і методи забезпечення безпеки. Засоби забезпечення інформаційної безпеки. Організаційно-технічне забезпечення комп'ютерної безпеки. Способи забезпечення інформаційної безпеки економічних систем. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення. Захист від комп'ютерних вірусів. Електронний цифровий підпис і особливості його застосування. Структура і задачі служби безпеки.

Захист інформації в Інтернеті.

Змістовний модуль 2. Інформаційна безпека окремих економічних систем.

Тема 4. Організація систем захисту інформації економічних систем.

Етапи побудови системи захисту інформації економічних систем. Політика безпеки економічних систем. Оцінка ефективності інвестицій в інформаційну безпеку. Визначення особливостей діяльності посадової особи залежно від класу автоматизованої інформаційної системи.

Тема 5. Інформаційна безпека систем на макроекономічному рівні.

Уточнення сутності основних категорій: "програмне забезпечення", "загальне програмне забезпечення", "специфічне програмне забезпечення", "інформаційна задача", "розрахункова задача". Характеристика структури програмного забезпечення електронної обчислювальної машини. Оцінка українських електронних баз «Дія», «Helsinki».

Тема 6. Інформаційна безпека автоматизованих банківських систем.

Забезпечення інформаційної безпеки банківських систем. Типи і суб'єкти загроз автоматизованих банківських систем. Система реєстрації та обліку. Контроль цілісності програмного забезпечення.

Тема 7. Інформаційна безпека електронної комерції.

Уточнення сутності основних категорій: "електронна комерція", "електронний каталог", "електронний універмаг". Складові інтернет-магазину, принципи його роботи. Технологія функціонування інтернет-магазину. Основні вимоги до проведення комерційних операцій. Проблеми в області безпеки електронного бізнесу. Загрози електронної комерції.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7

Змістовий модуль 1. Теоретичні основи інформаційної безпеки економічних систем.						
Тема 1. Основні аспекти інформаційної безпеки економічних систем.	18	4		4		10
Тема 2. Поняття інформаційних загроз та їх види.	18	4		4		10
Тема 3. Принципи побудови системи інформаційної безпеки.	22	6		6		10
Разом за змістовим модулем 1	58	14		14		30
Змістовий модуль 2. Інформаційна безпека окремих економічних систем.						
Тема 4. Організація систем захисту інформації економічних систем.	15	4		4		7
Тема 5. Інформаційна безпека систем на макроекономічному рівні.	16	4		4		8
Тема 6. Інформаційна безпека автоматизованих банківських систем.	15	4		4		7
Тема 7. Інформаційна безпека електронної комерції.	16	4		4		8
Разом за змістовим модулем 2	62	16		16		30
Усього годин	120	30		30		60

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Порівняльний аналіз стандартів інформаційної безпеки	4
2.	Види інформаційних загроз та засоби захисту інформації	4
3.	Побудова системи інформаційної безпеки	6
4.	Захист інформації від комп'ютерних вірусів та інших загроз	4
5.	Оцінка інформаційної безпеки систем національних систем	4
6.	Аналіз інформаційної безпеки банківських систем	4
7.	Організація захисту інформації в електронній комерції	4
	Разом	30

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Порівняльний аналіз стандартів інформаційної безпеки	10
2.	Види інформаційних загроз та засоби захисту інформації	10
3.	Побудова системи інформаційної безпеки	10
4.	Захист інформації від комп'ютерних вірусів та інших загроз	7
5.	Оцінка інформаційної безпеки систем національних систем	8

6.	Аналіз інформаційної безпеки банківських систем	7
7.	Організація захисту інформації в електронній комерції	8
	Разом	60

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами.

Перелік питань для визначення рівня засвоєння знань студентами

1. Необхідність забезпечення безпеки в інформаційних системах.
2. Прогрес інформаційних технологій та інформаційна безпека.
3. Нормативно-правові аспекти інформаційної безпеки.
4. Класифікація загроз безпеці інформаційних об'єктів.
5. Основні види каналів витоку інформації.
6. Природні небезпеки інформаційної безпеки.
7. Зовнішні небезпеки інформаційної безпеки.
8. Мотиви та цілі комп'ютерних злочинів.
9. Статті кримінального кодексу про комп'ютерні злочини
10. Кримінологічна характеристика злочинів у сфері комп'ютерної інформації та їх попередження.
11. Об'єкти інформаційної безпеки для підприємства.
12. Методи та засоби забезпечення інформаційної безпеки.
13. Організаційні методи забезпечення інформаційної безпеки.
14. Фізичний захист інформаційних систем.
15. Програмно – технічні методи забезпечення інформаційної безпеки.
16. Ідентифікація та аутентифікація.
17. Нормативні документи з інформаційної безпеки.
18. Несанкціонований доступ та захист від нього.
19. Проблема інформаційної безпеки у історичному аспекті.
20. Попередження комп'ютерних злочинів.
21. Типи комп'ютерних вірусів та захист від них.
22. Людські чинники, що зумовлюють інформаційні небезпеки.
23. Методи впливу загроз на інформаційний об'єкт.
24. Ознаки впливу вірусів на комп'ютерну систему.
25. Системний підхід захисту інформації.
26. Кримінально-правова характеристика комп'ютерних злочинів
27. Суб'єктивний бік комп'ютерних злочинів.
28. Об'єктивний бік комп'ютерних злочинів.
29. Способи скоєння комп'ютерних злочинів ("за хвіст", "маскарад" та ін.).
30. Причини та умови, що сприяють скоєнню комп'ютерних злочинів.
31. Заходи запобігання злочинам у сфері комп'ютерної інформації.
32. Історія шкідливих програм.

33. Захист облікової інформації комерційних фірм.
34. Властивості економічної інформації, що порушуються за несанкціонованого доступу.
35. Історичні аспекти комп'ютерних злочинів
36. Економічна інформація як об'єкт безпеки.
37. Перелік відомостей, які можуть становити комерційну таємницю.
38. Види таємниць та як їх зберегти.
39. Причини розголошення конфіденційної інформації.
40. Розголошення та витік інформації.
41. Стратегія зловмисника за несанкціонованого доступу.
42. Організація конфіденційного діловодства.
43. Структура служби безпеки компанії.
44. Теоретичні аспекти інформаційної безпеки економічних систем.
45. Основні поняття інформаційної безпеки економічних систем.
46. Економічна інформація як товар та об'єкт безпеки.
47. Поняття інформаційних загроз та їх види.
48. Інформаційні небезпеки.
49. Шкідливі програми.
50. Комп'ютерні злочини та покарання.
51. Принципи побудови системи інформаційної безпеки.
52. Державне регулювання інформаційної безпеки.
53. Підходи, принципи, методи та засоби забезпечення безпеки.
54. Організаційно-технічне забезпечення комп'ютерної безпеки.
55. Захист від комп'ютерних вірусів
56. Електронний цифровий підпис та особливості його застосування.
57. Захист інформації в Інтернеті.
58. Організація системи захисту інформації економічних систем.
59. Етапи побудови системи захисту.
60. Політика безпеки.
61. Оцінка ефективності інвестицій у інформаційну безпеку.
62. Забезпечення інформаційної безпеки автоматизованих банківських систем.
63. Інформаційна безпека електронної комерції
64. Забезпечення комп'ютерної безпеки облікової інформації.
65. Сутність криптографічних методів.
66. Організаційно-адміністративні заходи щодо забезпечення комп'ютерної безпеки.
67. Організація конфіденційного діловодства.
68. Принципи забезпечення інформаційної безпеки з урахуванням інженерно-технічного забезпечення.
69. Безпека електронної комерції

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

ОС Бакалавр Спеціальність 051 Економіка (Цифрова економіка)	Кафедра Економічної кібернетики	Екзаменаційний білет №7 з дисципліни «Інформаційна безпека економічних систем»	Затверджую: Зав кафедри проф. Жерліцин Д.М. _____ 2022 р.
1. Екзаменаційне питання (максимальна оцінка 10 балів за відповідь)			
Методи та засоби забезпечення безпеки економічних систем			
2. Задача (максимальна оцінка 10 балів за розв'язання задачі)			
Оцінити вигоду захисту інформації за наявності наступної інформації:			
<ul style="list-style-type: none"> - величина шкоди від загроз оцінена в \$5.000.000. - частота ситуації раз на три роки. - методи захисту спрацьовують у 65%. - витрати реалізації методів захисту становлять \$125.000. 			
3. Тестові завдання різних типів (максимальна оцінка 10 балів за відповідь на всі тестові завдання)			
Екзаменатор		доц. Негрей М.В.	

8. Методи навчання

В процесі викладання навчальної дисципліни за характером пізнавальної діяльності застосовуються переважно методи гейміфікації та пояснювально-ілюстративний, евристичний методи, метод демонстраційних прикладів, методи парної та групової роботи, а також частково кожен із зазначених методів залежно від видів робіт на занятті (Табл. 1).

Таблиця 1

Класифікація методів навчання

Засади	Найменування	Характеристики
1. Джерело знань: слово образ досвід	словесні, наочні, практичні	
2. Етапи навчання	підготовка до вивчення нового матеріалу, вивчення нового матеріалу, закріплення вправ, контроль і оцінка	
3. Спосіб педагогічного керівництва	пояснення педагога, самостійна робота	керівництво: безпосереднє; опосередковане
4. Стиль викладання (пояснення)	інформаційно-повідомлювальний, пояснювальний, інструктивно-	

	практичний, пояснювально-спонукальний	
4. Логіка навчання	індуктивні, дедуктивні, аналітичні, синтетичні	
5. Дидактичні цілі	організація навчальної діяльності, стимулювання і релаксація, контроль і оцінка	
6. Дидактичні завдання	методи оволодіння знаннями, методи формування умінь і навичок, застосування здобутих знань, умінь і навичок	
7. Характер пізнавальної діяльності	пояснювально- ілюстративні, репродуктивні проблемного викладу, частково-пошукові (евристичні), дослідницькі методи	репродуктивні продуктивні

При викладанні навчальної дисципліни використовуються такі методи навчання:

- М1. Лекція (дискусія, проблемна)
- М2. Лабораторна робота
- М3. Проблемне навчання
- М4. Проектне навчання(індивідуальне, малі групи, групове)
- М5. Он-лайн навчання

Та методи контролю:

- МК1. Тестування
- МК2. Контрольне завдання
- МК3. Розрахункова робота
- МК4. Методи усного контролю
- МК5. Екзамен

9. Форми контролю

Кожна з форм контролю має особливості й залежить від мети, змісту та характеру навчання. У процесі навчання дисципліни використовуються наступні форми контролю:

- **Поточний контроль:** усне опитування (індивідуальне, фронтальне, групове), комп'ютерне тестування, виконання практичних завдань на комп'ютері згідно програми;
- **Підсумковий контроль:** тестування та співбесіда за результатами роботи.

10. Розподіл балів, які отримують студенти. Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «Положення про екзамен та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371)

Поточний контроль		Рейтинг з навчальної роботи $R_{НР}$	Рейтинг з додаткової роботи $R_{ДР}$	Рейтинг штрафний $R_{ШТР}$	Підсумкова атестація (екзамен)	Загальна кількість балів
Змістовий модуль 1	Змістовий модуль 2					
0-100	0-100	0-70	0-20	0-5	0-30	0-100

Примітки.

Рейтинг з поточної роботи (навчальної, додаткової), штрафний рейтинг та показники підсумкової атестації визначаються відповідно п. 2 та п.4 Положення про екзамен та заліки у Національному університеті біоресурсів і природокористування України, що затверджене Вченою радою НУБіП України « 27 » грудня 2019 р. протокол №5.

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис} = R_{НР} + R_{ат}$.

Загальний рейтинг здобувача вищої освіти із засвоєння дисципліни у балах переводиться у національної оцінки наступним чином:

Шкала оцінювання: національна та ECTS

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

11. Методичне забезпечення

Електронний навчальний курс, розроблений на базі платформи LMS Moodle, розміщений на навчальному порталі НУБіП України за адресою: <https://elearn.nubip.edu.ua/course/view.php?id=4714>

12. Рекомендована література

Основна

1. Інформаційна безпека / Навч.посіб. За ред. Бобала Ю.Я., Горбатого І.В. – Львів: Львівська політехніка, 2019, 580 с.
2. Лизанчук В. Інформаційна безпека України: теорія і практика. – Львів: ЛНУ ім. Івана Франка, 2017, 728 с.
3. Фармагей О., Мельник Д., Петрик В., Карпович О., Остроухов В., Присяжнюк М., Чеховська М. Інформаційна безпека. – К.: Ліра-К, 2021, 412 с.

Додаткова література

4. Snishchenko, R., & Grynychutskyi, V. (2020). Інформаційна безпека як складова економічної безпеки суб'єктів господарювання. Економічний аналіз, 30(1 (1)), 241-248.
5. Бехтер Л. А. Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств. Агросвіт. 2020. № 12. С. 66–70. DOI: 10.32702/2306-6792.2020.12.66
6. Вашай, Ю.В. Гармонізація інформаційно-аналітичного забезпечення управління економічною безпекою держави в умовах військово-політичної нестабільності: монографія / Вашай Ю. В., Дорошенко О. О. ; Нац. ун-т вод. госп-ва та природокористування. - Рівне : НУВГП, 2020. - 109 с.
7. Гладких, Д. М. Банківська безпека держави в умовах розвитку інформаційної економіки (трансформації банківських операцій) : [монографія] / Д. М. Гладких ; Нац. ін-т стратег. дослідж. - Київ : НУОУ, 2019. - 392 с.
8. Дейнега, О. В. (2019). Інформаційна безпека підприємств в умовах глобалізації 4.0. Економіка та суспільство, 2019(Вип. 20), 199-208.
9. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003р. №851-IV. Режим доступу : <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15>.
10. Закон України “Про захист персональних даних” від 01.06.2010р. № 2297-VI/ Режим доступу : <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17>
11. Закон України “Про інформацію” від 02.10.1992р. № 2657-XII. Режим доступу : <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12>.
12. Кіндзерський Ю.В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. Економічний вісник Дніпровської політехніки. 2020. Вип. 3 (71). С. 18–26.

13. Концепція інформаційної безпеки України. URL: [http://mir.gov.ua/files/banners/Final%20Проект%20концепції%20\(Текст\)%20-%2030.09.15.pdf](http://mir.gov.ua/files/banners/Final%20Проект%20концепції%20(Текст)%20-%2030.09.15.pdf)
14. Місюкевич В. І., Трушкіна Н. В., Шкригун Ю. О. Електронна комерція у глобальному цифровому просторі: нові виклики та напрями розвитку / Формування системи внутрішньої торгівлі України: теорія, практика, інновації : колективна монографія / за ред. В. В. Лісіци, В. І. Місюкевич, О. М. Михайленко. Полтава : ПУЕТ, 2020. 361 с.
15. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. Автоматизация технологических и бизнес-процессов. 2017. № 9(2). С. 36-42.
16. Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>.
17. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України : наказ Міністерства економіки України; від 23.10.2013 р. № 1277. URL: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>.
18. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
19. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text>.
20. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.
21. Фісуненко, П. А., Судакова, О. І., Деркач, С. В., & Притуляк, Є. О. (2019). Методологічні аспекти забезпечення інформаційної безпеки підприємства. Східна Європа: економіка, бізнес та управління, 426-431.

13. Інформаційні ресурси

22. World Bank Open Data. Режим доступу: <https://data.worldbank.org>
23. World Economic Forum Режим доступу: <https://www.weforum.org/>
24. Міністерство Фінансів України. Режим доступу: <https://www.minfin.gov.ua/>
25. Національний банк України. Режим доступу: <https://bank.gov.ua/control/uk/index>
26. Організація економічного співробітництва та розвитку. Режим доступу: <https://data.oecd.org>

27. Державна служба статистики України [Електронний ресурс] / Режим доступу: <http://www.ukrstat.gov.ua/>

28. Державна комісія з регулювання ринків фінансових послуг України [Електронний ресурс] / Режим доступу: <http://www.dfp.gov.ua>

29. Національний банк України [Електронний ресурс] / Режим доступу: <http://www.bank.gov.ua>

30. ПФТС Фондова біржа [Електронний ресурс] / Режим доступу: <http://pfts.com.ua>