МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КІБЕРГІГІЄНИ

Назва освітньо-професійної програми	Комп’ютерні науки
Рівень вищої освіти	перший (бакалаврський) рівень
Галузь знань	F Інформаційні технології
Спеціальність	F3 Комп’ютерні науки
Вид навчальної дисципліни	обов’язкова
Мова викладання	українська
Рік навчання	перший (заочна)

2025

ЗАТВЕРДЖЕНО
Науково-методичною радою
Дніпровського державного
університету внутрішніх справ
протокол від 11.07.2025№ 11

ПОГОДЖЕНО
Гарант освітньої програми «Комп'ютерні науки»

Юлія СИНИЦІНА

Розглянуто на засіданні кафедри Інформаційних технологій
Протокол від 30.06.2022 № 21.

Основи кібергігієни. Робоча програма навчальної дисципліни. Дніпро: Дніпровський державний університет внутрішніх справ, 2025 рік. кількість сторінок 14 с.

РОЗРОБНИК:
Доцент кафедри інформаційних технологій, кандидат технічних наук, доцент,
Синиціна Юлія Петрівна

РЕЦЕНЗЕНТИ:
1. Професор кафедри інформаційних технологій і систем Українського державного університету науки і технологій, доктор технічних наук, професор, Гуда Антон Ігорович;
2. Доцент кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка», кандидат технічних наук, доцент, Станіна Ольга Дмитрівна

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни
(додаток 1 до Робочої програми навчальної дисципліни)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Характеристика навчальної дисципліни	
	денна форма здобуття вищої освіти	заочна форма здобуття вищої освіти
Кількість кредитів ЄКТС		4
Загальна кількість годин		120
Рік підготовки		перший
Семестр		1
Лекції		2
Семінарські		
Практичні		8
Самостійна робота		110
Індивідуальні завдання (курсова робота)		–
Підсумковий семестровий контроль		екзамен

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Основи кібергігієни» є формування у здобувачів вищої освіти цілісного уявлення про принципи, методи та інструменти забезпечення особистої та корпоративної безпеки в кіберпросторі. Дисципліна покликана ознайомити з основними кіберзагрозами та їхніми наслідками, а також навчити розпізнавати їх і протидіяти..

Очікувані результати навчання:

знати:

– основні поняття кібергігієни, інформаційної безпеки та захисту персональних даних;

– основні кіберзагрози (шкідливе ПЗ, фішинг, соціальна інженерія, кібершахрайство) та методи їх запобігання;

– принципи безпечної роботи в мережі Інтернет та використання цифрових сервісів;

– основи політик безпеки в організаціях та законодавчі аспекти захисту інформації;

– правила створення та використання надійних паролів і двофакторної аутентифікації;

– основи етичного використання інформаційних технологій та принципи цифрової культури.

вміти:

– оцінювати рівень власної кібергігієни та визначати потенційні ризики у цифровому середовищі;

– застосовувати базові заходи захисту інформації (антивірусні програми, шифрування, резервне копіювання);

– користуватися інструментами безпечного доступу до ресурсів Інтернету та хмарних сервісів;

– ідентифікувати та реагувати на потенційні кібератаки та підозрілі дії у мережі;

– дотримуватися правил безпечного обміну інформацією та цифрової етики у навчальній і професійній діяльності;

– аналізувати сучасні тенденції у сфері кібербезпеки та пропонувати заходи щодо підвищення кібергігієни у колективних проєктах.

Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою: Комп'ютерні науки.

Інтегральна компетентність – здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК1 – Здатність до абстрактного мислення, аналізу та синтезу.

ЗК3 – Знання та розуміння предметної області та розуміння професійної діяльності.

Спеціальні компетентності:

СК14 – Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК17 – Здатність забезпечувати безпеку інформаційних систем та мереж, розробляти та впроваджувати засоби захисту інформації, аналізувати та управляти ризиками в інформаційній безпеці.

СК18 – Володіння сучасними методами захисту інформації, розуміння принципів роботи алгоритмів шифрування, блокчейн-технологій та їх застосування у комп'ютерних системах.

Пререквізити та постреквізити дисципліни:

Постреквізити: «Операційні системи та їх адміністрування», «Комп'ютерні мережі та їх безпека», «Технології комп'ютерного проєктування та об'єктно-орієнтоване програмування». «Адміністрування та організація сучасних обчислювальних систем», «Інформаційні системи та технології. Технології захисту даних», «Бази даних та технології захисту баз даних».

Здобувачі вищої освіти повинні продемонструвати такі **результати навчання**:

РН16 – Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

РН18 – Здатність проєктувати та впроваджувати безпечні інформаційні системи; проектувати архітектуру інформаційних систем з урахуванням вимог захисту конфіденційної інформації.

РН19 – Здатність ідентифікувати, оцінювати та запобігати загрозам інформаційної безпеки та розробляти ефективні заходи протидії, використовуючи сучасні інструменти та методики інформаційної безпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1. ВСТУП ДО КІБЕРГІГІЄНИ ТА ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Поняття кібергігієни та її значення для сучасного користувача. Основні кіберзагрози та їх класифікація. Принципи безпечного використання персональних пристроїв і мережі Інтернет.

ТЕМА 2. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВИХ ОБЛІКОВИХ ЗАПИСІВ.

Основи створення надійних паролів та двофакторної аутентифікації. Політика приватності в соціальних мережах та хмарних сервісах. Шифрування даних та безпечне зберігання інформації.

ТЕМА 3. КІБЕРЗАГРОЗИ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ.

Види шкідливого ПЗ (віруси, трояни, шпигунські програми). Фішинг, соціальна інженерія та шахрайство в Інтернеті. Антивірусний захист та принципи оновлення програмного забезпечення.

ТЕМА 4. ПОШУК ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ. ОСОБИСТА БЕЗПЕКА В ІНТЕРНЕТІ.

Історія розвитку та загальна характеристика пошукових систем. Пошук інформації за допомогою GOOGLE: сервіси, спеціальний пошук, апаратне забезпечення та інструменти. Мета-пошукові системи та системи анонімного пошуку інформації. Пошук оперативної інформації в соціальних мережах Facebook. Застосування чат-ботів у месенджері Telegram. Особиста безпека у інтернеті.

4. СТРУКТУРА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАОЧНА ФОРМА НАВЧАННЯ

Теми та план лекційних занять

Назва теми лекційного заняття	План лекційного заняття	Кількість годин
Тема № 1. Вступ до кібергігієни та основи інформаційної безпеки.	1. Поняття кібергігієни та її значення для сучасного користувача. 2. Основні кіберзагрози та їх класифікація. 3.Принципи безпечного використання персональних пристроїв і мережі Інтернет.	2

Теми практичних занять

Назва теми практичних занять	Кількість годин
Тема № 1. Вступ до кібергігієни та основи інформаційної безпеки.	2
Тема № 2. Захист персональних даних та цифрових облікових записів.	2
Тема № 3. Кіберзагрози та методи їх запобігання.	2
Тема № 4. Пошук інформації в мережі інтернет. особиста безпека в інтернеті.	2

Теми для самостійної роботи

Назва теми для самостійної роботи	Кількість годин
Тема № 1. Вступ до кібергігієни та основи інформаційної безпеки.	28
Тема № 2. Захист персональних даних та цифрових облікових записів.	32
Тема № 3. Кіберзагрози та методи їх запобігання.	18
Тема № 4. Пошук інформації в мережі інтернет. особиста безпека в інтернеті.	32

5. ПЕРЕЛІК ПИТАНЬ ТА ЗАВДАНЬ, ЩО ВИНОСЯТЬСЯ НА ПІДСУМКОВИЙ КОНТРОЛЬ

1. Що таке кібергігієна і чому вона важлива для сучасного користувача?
2. Назвіть основні складові кібергігієни.
3. Які основні кіберзагрози існують у сучасному цифровому середовищі?
4. Наведіть приклади фізичних і цифрових загроз для персональних пристроїв.
5. Які принципи безпечного використання персональних пристроїв слід дотримуватися?
6. Поясніть поняття «інформаційна безпека» та її основні цілі.
7. Які наслідки можуть бути у разі порушення кібергігієни?
8. Що таке надійний пароль і які правила його створення?
9. Навіщо потрібна двофакторна аутентифікація (2FA)?
10. Назвіть види двофакторної аутентифікації.
11. Які основні загрози існують у соціальних мережах щодо персональних даних?
12. Що таке політика приватності у хмарних сервісах?
13. Наведіть приклади методів шифрування даних.
14. Як безпечно зберігати інформацію на персональному пристрої та у хмарі?

15. Які ризики виникають при використанні однакових паролів на різних сервісах?
16. Яким чином можна перевірити надійність свого пароля?
17. Назвіть основні види шкідливого програмного забезпечення.
18. В чому відмінність вірусу, трояна і шпигунської програми?
19. Що таке фішинг і як його розпізнати?
20. Поясніть поняття «соціальна інженерія» та наведіть приклади.
21. Які основні принципи антивірусного захисту?
22. Чому важливо регулярно оновлювати програмне забезпечення?
23. Назвіть приклади безпечної поведінки у мережі для запобігання кібератакам.
24. Як можна перевірити, що файл чи посилання безпечні перед відкриттям?
25. Як розвивалася історія пошукових систем та які основні етапи їх розвитку?
26. Назвіть основні сервіси Google, що використовуються для пошуку інформації.
27. Що таке мета-пошукові системи і чим вони відрізняються від звичайних?
28. Як забезпечити анонімний пошук інформації в Інтернеті?
29. Як шукати оперативну інформацію у Facebook та інших соціальних мережах?
30. Які основні правила особистої безпеки під час користування Інтернетом та чат-ботами в месенджерах, таких як Telegram?

6. КРИТЕРІЇ ТА ЗАСОБИ ОЦІНЮВАННЯ УСПІШНОСТІ НАВЧАННЯ

ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота/ Індивідуальна робота	Екзамен (Е)
≤ 20	≤ 30	
≤ 50		≤ 50
Підсумкова оцінка у випадку екзамену (П) = ПК + Е ≤ 100		

Критерієм успішного проходження Здобувачем підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Мінімальний пороговий рівень оцінки визначається за допомогою якісних критеріїв і трансформується в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Здобувач допускається до складання підсумкового контролю, якщо ним виконані всі передбачені РПНД поточні завдання та сума балів поточного контролю не менше ніж 34. Якщо сума балів поточного контролю менше ніж 34, здобувач не допускається до підсумкового контролю і зобов’язаний доопрацювати завдання та набрати необхідну кількість балів.

За результатами аудиторної роботи здобувач заочної форми навчання має отримати максимальну кількість 20 балів (кожне заняття оцінюється за п’ятибальною шкалою); за результатами самостійної роботи – 30 балів. Таким чином бали за поточний контроль (34-50 балів).

Розрахунок підсумкової оцінки з навчальної дисципліни «Основи кібергігієни» здійснюється відповідно до формули:

П=ПК+Е≤100,

де ПК – бали за поточний контроль (34-50 балів),

З – бали за результатами складання екзамену

Критерії оцінювання аудиторної роботи здобувачів вищої освіти (денна та заочна форми навчання)

БАЛИ	ПОЯСНЕННЯ
5	**Високий рівень** компетентностей. Питання, винесені на розгляд, засвоєні у повному обсязі; на високому рівні сформовані необхідні практичні навички та вміння; всі навчальні завдання, передбачені планом заняття, виконані в повному обсязі. Під час заняття продемонстрована стабільна активність та ініціативність. Відповіді на теоретичні питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань ґрунтується на глибокому знанні систем та методів інформаційної підтримки діяльності Національної поліції.
4	**Невисокий рівень** компетентностей. Питання, винесені на розгляд, засвоєні у повному обсязі; в основному сформовані необхідні практичні навички та вміння; всі передбачені планом заняття навчальні завдання виконані в повному обсязі з неістотними неточностями. Під час заняття продемонстрована ініціативність. Відповіді на питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань переважно ґрунтується на знанні систем та методів інформаційної підтримки діяльності Національної поліції.
3	**Достатній рівень** компетентностей. Питання, винесені на розгляд, у цілому засвоєні; практичні навички та вміння мають поверхневий характер, потребують подальшого напрацювання та закріплення; навчальні завдання, передбачені планом заняття, виконані, деякі види завдань виконані з помилками.
2	**Недостатній рівень** компетентностей Питання, винесені на розгляд, засвоєні частково, прогалини у знаннях не носять істотного характеру; практичні навички та вміння сформовані недостатньо; більшість навчальних завдань виконано, деякі з виконаних завдань містять істотні помилки, які потребують подальшого усунення.
1	**Мінімальний рівень** компетентностей. Студент не готовий до заняття, не знає більшої частини програмного матеріалу, з труднощами виконує завдання, невпевнено відтворює терміни і поняття, що розглядалися під час заняття, допускає змістовні помилки, не володіє відповідними вміннями і навичками, необхідними для розв'язання професійних завдань.
0	**Незадовільний рівень** компетентностей. Відсутність на занятті.

Для навчальної дисципліни «Основи кібергігієни» засобами діагностики знань (успішності навчання) виступають: стандартизовані тести, тези, есе, презентації результатів виконаних завдань та досліджень, презентації та виступи на наукових заходах, інші види індивідуальних та групових завдань.

Критерії оцінювання самостійної роботи (заочна форма навчання)

Пропонується наступне оцінювання самостійної роботи здобувачів за виконання 1 завдання за вибором здобувача та узгодженням з викладачем для отримання максимальної кількості балів - 30:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед здобувачів, (МОН, ДДУВС) (написання робіт, есе, доповідь, творча публікація, творча візуалізація, відеоролик) - 30 балів.
2. Підготовка презентацій-доповідей участі в роботі науковому студентську гуртку кафедри (надати презентація та фото виступу) – 30 балів.
3. Підготовка тези доповідей на міжнародну (всеукраїнську) науково-практичну конференцію за умови надання PrinScrin перевірки на плагіат за результатом не менше 70% оригінального тексту. Тези повинні бути підготовленні відповідно «Методичних вказівок з написання тез» – 30 балів.
4. Отримання сертифікату після проходження курсу «Основи кібергігієни» Освітній серіал. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene - 30 балів.
5. Виконання індивідуальної роботи згідно завдання викладача (до 10 балів: Кросворд – 3 балів; Реферат – 3 балів; Есе – 4 балів).
6. Проходження тесту з самостійної роботи - 30 балів.

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ECTS	
	Залік	Екзамен/ диференційований залік	Оцінка	Пояснення
90-100	зараховано	Відмінно	A	«**Відмінно**» - теоретичний зміст курсу засвоєний у повному обсязі; сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані в повному обсязі.
83-89		Добре	B	«**Дуже добре**» - теоретичний зміст курсу засвоєний в повному обсязі; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання більшості з них оцінена кількістю балів, близько до максимальної.
75-82			C	«**Добре**» - теоретичний зміст курсу засвоєний цілком; в основному сформовані практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання жодного з них не оцінена мінімальною кількістю балів, деякі види завдань виконані з помилками.
68-74		Задовільно	D	«**Задовільно**» - теоретичний зміст курсу засвоєний не повністю; але прогалини не носять істотного характеру; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; більшість передбачених РПНД навчальних завдань виконано, деякі з виконаних завдань містять помилки.
60-67			E	«**Достатньо**» - теоретичний зміст курсу засвоєний частково; не сформовано деякі практичні навички роботи; частина передбачених РПНД навчальних завдань не виконані або якість виконання деяких з них оцінено числом балів, близьким до мінімального.
35-59	не зараховано	Не задовільно	FX	«**Умовно незадовільно**» - теоретичний зміст курсу засвоєний частково; не сформовані необхідні практичні навички роботи; більшість навчальних завдань не виконано або якість їх виконання оцінено кількістю балів, близько до мінімальної; при додатковій самостійній роботі над матеріалом курсу можливе

				підвищення якості виконання навчальних завдань (з можливістю повторного складання).
1-34			F	«**Безумовно незадовільно**» - теоретичний зміст курсу не засвоєний; не сформовані необхідні практичні навички роботи; всі виконані навчальні завдання містять грубі помилки або не виконані взагалі; додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань.

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧЕНО НАВЧАЛЬНОЮ ДИСЦИПЛІНОЮ

1. Комп'ютерна техніка, відповідне програмне забезпечення.
2. Наявність доступу до Інтернет.
3. Мультимедійне обладнання.

8. ІНФОРМАЦІЙНЕ ТА МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ (рекомендовані джерела інформації)

Основні нормативні акти:

- закони:

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 20.07.2025);
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 20.07.2025).
3. Про критичну інфраструктуру: Закон України від 16.11.2021. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
5. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021, введено в дію Указом Президента України від 19.03.2021 № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.

- постанови, інші рішення, роз'яснення суддів (Конституційного, Верховного):

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних система: Постанова КМУ від 8 лютого 2021 року № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text;
2. Про затвердження Положення про інформаційно-комунікаційну систему

«Інформаційний портал Національної поліції України»: Наказ МВС України від 03.08.2017 № 676. Дата оновлення: 01.04.2022. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

Підручники:

1. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл.
URL: https://univd.edu.ua/science-issue/issue/4315.
2. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В.Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с.
URI: https://er.dduvs.in.ua/handle/123456789/7110;
3. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: Дніп-роп. держ. ун-т внутр.справ, 2021. 492с. URI: http://er.dduvs.in.ua/handle/123456789/6820.

Навчальні посібники, інші дидактичні та методичні матеріали:

1. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с.
URI: https://er.dduvs.edu.ua/handle/123456789/15045.
2. Інформаційні та комунікаційні технології: навч. посіб. / А. М. Гребенюк, Е. В. Рижков Ю. П. Синиціна, С. О. Прокопов. – Дніпро: ДДУВС, 2024. – 337 с.
URI: https://er.dduvs.edu.ua/handle/123456789/14223.
3. Бутенко Т.А. Сирий В.М. Інформаційні системи та технології : навчальний посібник - Харків: ХНАУ ім. В.В. Докучаєва, 2020. 207 с.
4. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
5. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

Монографії та інші наукові видання:

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. Захист інформаційних ресурсів підрозділів Національної поліції місцевого рівня: методичні рекомендації / О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2018. 34 с.;
3. Синиціна Ю.П., Станіна О.Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Rationale for the relevance of digital communication in higher education institutions) Міжн. колект.моногр. / Selected aspects of digital society development «Digital Economyand Digital Society» III

Міжнародна конференція (28-29 травня 2021 р.) – Katowice, University of Technology, Poland, 2021.mon # 45 – 148- 156 с ISBN 978 – 83 – 960717 – 1 – 2.;
4. Синиціна Ю.П., Рижков Е.В., Станіна О.Д. Штучний інтелект: що змінилося за 50 років. Theoretical foundations of engineering. Tasks and problems: collective monograph / Boiko T., Boiko P., – etc. – International Science Group. – Boston : Primedia eLaunch, 2021. 485 p. Available at : DOI-10.46299/ISG.2021.MONO.44TECH.III
5. Синиціна Ю.П., Бекишев А. Методологічні аспекти цифрової комунікації закладів вищої освіти Науковий вісник, м. Дніпро, 2021, № 3, С. 340-348; ISSN – 2078-3566; «Index Copernicus International» «CrossRef», DOI: 10.31733/2078-3566-2021-3-340-348

Інші джерела:

1. Ковальова О. В. Інформаційне забезпечення професійної діяльності: навч. посіб. Київ: «Дакор», 2021. 288 с.;
2. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с.
3. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
4. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
5. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3030-03638-6_18).
6. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. Journal of Homeland Security and Emergency Management. 2014. Vol. 11. Iss. 4. pp. 489–510. (DOI: 10.1515/ jhsem-2014-0035).
7. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.
8. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160)
9. Синиціна Ю.П., Причина В.Р. Оцінка системи управління інформаційної безпеки методом таксономії Nauka i edukacja w warunkach zmian cywilizacyjnych: Mater. II Międz. Konf. Nauk.-Prakt. / Pod red. Stanisława Kowalczyka – Łódź: Nowa nauka, 2020, p. 76 – 78 ISBN 978-83-7364-968-2;
10.Синиціна Ю.П. APT-атак – пріоритетний напрямок розвитку кібербезпеки Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. 19.12. 2020 р., м. Львів : ЛьвДУВС, 2020. с. 66-68;

11.Синиціна Ю.П. Сучасні підходи до безпеки операційних систем Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро:ДДУВС, 2020. с. 66-68;
12.Синиціна Ю.П., Дудуник В.В. Актуальні питання взаємозв'язку інформаційної та національної безпеки України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро:ДДУВС, 2020. с. 164-167;
13.Синиціна Ю.П., Кліменко А.О. Актуальні питання інформаційної безпеки в діяльності Національної поліції України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро:ДДУВС, 2020. с. 174-1764
14.Синиціна Ю.П. Автоматизовані інформаційні системи в правоохоронній діяльності Економічна та інформаційна безпека: актуальні питання та інновації: Всеукр. наук.-практ. конф. (м. Дніпро, 04 листопада 2021 р.,). Дніпро: ДДУВС, 2021. С. 220-222;
15.Синиціна Ю.П. Державного управління забезпечення національної безпеки: інформаційна безпека Міжнародна та національна безпека: теоретичні і прикладні аспекти: VI Міжн. наук.-практ. конф. м. Дніпро, 11 березня 2022р.,). Дніпро: ДДУВС, 2022. С. 263 -266;
16.Синиціна Ю.П. Інформаційна безпека у системі права національної безпеки України Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об'єктів права інтелектуальної власності: зб. наук.праць за матеріал. IV Міжн. наук.-практ. інтер.-конф. (24-25 березня 2022р.). УДУНТ, УКРНЕТ, НДІІВ НАПрН України, Дніпро: Юрсервіс, 2022. С. 165 – 168.

Інтернет-ресурси:

1. Інформаційно-пошукова правова система «Нормативні акти України» (НАУ): http://www.nau.ua
2. Офіційний сайт Єдиного державного веб-порталу відкритих даних: https://data.gov.ua/
3. Бібліотека ХНУВС. URL: https://lib.univd.edu.ua/
4. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Т.в.о. завідувача кафедри
інформаційних технологій **Юлія СИНИЦІНА**

Додаток 1 до Робочої програми
навчальної дисципліни

Лист оновлення та перезатвердження робочої програми навчальної дисципліни

Навчальний рік	Протокол та дата засідання кафедри	Зміст змін	Підпис завідувача кафедри