|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ПРАВОВЕ РЕГУЛЮВАННЯ ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ**  СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ | | | | | |
| **Шифр і назва спеціальності** | | | 035 Філологія | **Факультет** | Соціально-гуманітарних технологій |
| **Назва програми** | | | Прикладна та комп’ютерна лінгвістика | **Кафедра** | ПРАВА |
| **Тип програми** | | | Освітньо-професійна | **Мова навчання** | українська |
| **Викладач** | | | | | |
| *Перевалова Людмила Вікторівна, Liudmyla.Perevalova@khpi.edu.ua* | | | | | |
|  | | Кандидат філософських наук, доцент,професор кафедри права НТУ «ХПІ», автор понад 150 наукових та науково-методичних праць. Провідний лектор з дисципліни: «Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві» | | | |
| **Загальна інформація про навчальну дисципліну** | | | | | |
| **Анотація** | | В рамках курсу викладаються основні поняття інформаційної безпеки держави. Надається класифікація загроз для інформаційної безпеки держави, суспільства та особи. Визначаються особливості та основні форми інформаційного протиборства. Викладено загальні поняття безпеки інформаційних ресурсів. Розглянуті способи побудови інформаційно-комунікаційних систем і мереж на основі сучасних способів передачі й обробки інформації та способи захисту інформації в інформаційних системах і мережах. Аналізується політика та система забезпечення інформаційної безпеки України. Надається характеристика нормативно-правових актів України та міжнародно-правових документів, які сприяють забезпеченню інформаційної безпеки України. | | | |
| **Цілі навчальної дисципліни** | | Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві є формування у майбутніх фахівців розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки особистості, держави, суспільства. | | | |
| **Формат** | | Лекції, семінарські заняття, самостійна робота, консультації. Підсумковий контроль – залік. | | | |
| **Семестр** | П’ятий | | | | |

**Компетентності:**

Загальні компетентності

ЗК-4. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні

**Результати навчання:**

Програмні результати навчання за спеціальністю

РН-3. Знати правове забезпечення охорони природного навколишнього середовища, вміти проводити інструментальні виміри числових значень нормованих показників стану навколишнього та виробничого середовища. ▪ РН-4. Здобуття навичок побудови правової позиції з різних питань застосування законодавства та її юридичної аргументації.

**Теми, що розглядаються:**

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи

Тема 2. Інформаційна безпека та кібербезпека.

Тема 3. Загрози для інформаційної безпеки держави, суспільства, людини

Тема 4. Принципи, форми та методи забезпечення інформаційної безпеки держави

Тема 5. Інформаційне протиборство між країнами. Інформаційна війна

Тема 6. Інформаційна зброя в інформаційні війні

Тема 7. Основи теорії інформаційної боротьби

Тема 8. Основи безпеки інформаційних ресурсів

Тема 9. Забезпечення безпеки інформації та інформаційних ресурсів

Тема 10. Захист інформаційних систем

Тема 11. Інформаційна безпека України

**Форма та методи навчання**

Під час проведення занять з навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві» використовуються такі методи навчання як: лекції, інноваційні методи з використанням мультимедійних презентацій, співбесіда, пояснення, ділова гра, вирішення конкретних правових ситуацій.

**МЕТОДИ КОНТРОЛЮ**

(надається опис методів контролю)

Перевірка та оцінювання знань студентів за дисципліною проводиться наступними методами:

1. Оцінювання активності студента під час лекційних занять.

2. Написання та презентація реферату.

3. Перевірка самостійної роботи студентів.

4. Проведення заліку.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

* з лекційного матеріалу – шляхом перевірки конспектів;
* з індивідуальних завдань – за допомогою перевірки самостійної роботи: тестів, задач, заслуховування рефератів з презентаціями.

Семестровий контроль проводиться у формі заліку (з оцінкою) відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

**РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)**

Максимальна сума балів, що може бути набрана студентом за результатами поточного контролю з навчальної дисципліни, складає 100 балів.

Кількість балів за контрольну роботу визначаються з урахуванням складності, обсягу та значущості в засвоєнні дисципліни (таблиця 1).

В таблиці 1 наведений приклад тих пунктів за якими студент накопичує бали, ці пункти можуть відрізнятися та розглядаються індивідуально для конкретної дисципліни.

Таблиця 1. – Розподіл балів для оцінювання успішності студента

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Поточний контроль | Контроль самостійної роботи | План-конспект заняття | Залік | Сума |
| 15 | 15 | 15 | 55 | 100 |

**Критерії та система оцінювання знань та вмінь студентів.**

Згідно основних положень ЄКТС, під системою оцінювання слід розуміти сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними критеріями оцінювання для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

**Критерії оцінювання –** це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв’язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.
2. Підвищення об’єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100-бальної шкали (табл. 2). Оцінки обов’язково переводять у національну шкалу (з виставленням державної семестрової оцінки «відмінно», «добре», «задовільно» чи «незадовільно») та у шкалу ЕСТS (А, В, С, D, Е, FХ, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЕСТS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Рейтинго-ва оцінка, бали** | **Оцінка ЕСТS та її визна-чення** | **Націо-**  **нальнаоцінка** | **Критерії оцінювання** | |
| **позитивні** | **негативні** |
| 1 | 2 | 3 | 4 | 5 |
| 90-100 | А | Відмінно | - **глибоке знання** навчального матеріалу модуля, що містяться в **основних і додаткових літературних джерелах;**  - **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв’язку і розвитку;  - **вміння** проводити **теоретичні розрахунки**;  - **відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;**  **- вміння вирішувати складні практичні задачі.** | - відповіді на запитання можуть містити **незначні неточності** |
| 82-89 | В | Добре | - **глибокий рівень знань** в обсязі **обов’язкового матеріалу**, що передбачений модулем;  - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;  - вміння вирішувати **складні практичні задачі.** | - відповіді на запитання містять **певні неточності** |
| 75-81 | С | Добре | - м**іцні знання** матеріалу, що вивчається, та його **практичного застосування;**  **-** вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**;  - вміння вирішувати **практичні задачі.** | **-** невміння використовувати теоретичні знання для вирішення **складних практичних задач** |
| 64-74 | D | Задовільно | - знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**;  - вміння вирішувати прості **практичні задачі**. | - невміння давати **аргументовані відповіді** на запитання;  - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;**  - невміння вирішувати **складні практичні задачі.** |
| 1 | 2 | 3 | 4 | 5 |
| 60-63 | Е | Задовільно | - знання **основних фундаментальних положень** матеріалу модуля,  - вміння вирішувати найпростіші **практичні задачі**. | - незнання **окремих (непринципових) питань** з матеріалу модуля;  - невміння **послідовно і аргументовано** висловлювати думку;  - невміння застосовувати теоретичні положення при розв’язанні **практичних задач** |
| 35-59 | FХ  (потрібне додаткове вивчення) | Незадо-вільно | **- додаткове вивчення** матеріалу модуля може бути виконане **в терміни, що передбачені навчальним планом**. | - незнання **основних фундаментальних положень** навчального матеріалу модуля;  - **істотні помилки** у відповідях на запитання;  - невміння розв’язувати **прості практичні задачі** |
| 1-34 | F  (потрібне повторне вивчення) | Незадо-вільно | – | - повна **відсутність знань** значної частини навчального матеріалу модуля;  - **істотні помилки** у відповідях на запитання;  -незнання основних фундаментальних положень;  - невміння орієнтуватися під час розв’язання **простих практичних задач** |

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Конституція України // Відомості ВРУ, 1996, №30, ст..141, [Електронний ресурс]. Режим доступу:

<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-ІV. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>

3. Про інформацію: Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

4. Про національну безпеку України: Закон України// Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України// Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

6. Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

7. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України// Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>

8. Резолюция 60/45, принятая Генеральной Ассамблеей ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». [Електронний ресурс]. Режим доступу:

<https://zakon.rada.gov.ua/laws/show/995_e45#Text>

9. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі». [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_243#Text>

10. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» от 03.12.2013. [Електронний ресурс]. Режим доступу: <https://www.osce.org/files/f/documents/0/a/109648.pdf>

11. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/995_266#Text>

12. Верголяс О.О. Міжнародно-правове регулювання інформаційного протиборства: реалії та перспективи. Visegrad Journalon Human Rights. 2019. №3. C. 58-63

13. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с.

14. Ємельянов В. М. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України / В. М. Ємельянов, Г. Л. Бондар // Публічне управління та регіональний розвиток. – 2019. – № 5. – С. 493-523.

15. Інформаційна безпека держави: підручник: в 2 т. Т. 1. / В.М. Петрик та ін.; за заг. ред. В.В. Остроухова. Київ: ДНУ «Книжкова палата України», 2016. 264 с.

16. Інформаційна безпека / За ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Вид-во Львівської політехніки. 2019. 580 с.

17. Історія інформаційно-психологічного протиборства: підруч./ [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.

18. Кіберзлочини в Україні (кримінально-правова характеристика) [Текст] : навч. посіб. / А. В. Боровик, І. М. Копотун. - Луцьк : Волинь Поліграф, 2019. - 304 с.

19. Корпоративна безпека: практичний посібник. Консалтингова компанія Сідкон. 2018. 276 с.

20. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON. 2021. 372 с.

21. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с.

21. Лизанчук В. Інформаційна безпека України: теорія і практика. Львів. Вид-во ЛНУ ім. Івана Франка. 2017. 728 с.

23. Мехед Д., Ткач Ю., Базилевич В., Гур’єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. Захист інформації. 2018. № 1. С. 61 – 66.

24. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті: навч.-метод. посібник / за ред. О. В. Лісового та ін. – К., 2018. – 105 с.

25. Нашинець-Наумова А.Ю. Інформаційна безпека суб’єктів господарювання: проблеми теорії та практики правозастосування: Монографія. Видав. Дім «Гельветика». 2017. 386 с.

26. Петрик В., Присяжнюк М. Інформаційна безпека держави. Підручник у 2-х томах. Київ. Вид-во «Книжкова палата України». 2016. 264 с.

27. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім «Києво-Могилянська академія», 2015. – 497 с.

28. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.

29. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім «Києво-Могилянська академія», 2015. – 497 с.

30. Харитонов Є.О., Давидова І.В. Інформаційна безпека: проблеми приватного права. Навч.- методичний посібник. Вид-во Фенікс, 2020. 194 с.

**Структурно-логічна схема вивчення навчальної дисципліни**

Таблиця 3. – Перелік дисциплін

|  |  |
| --- | --- |
| Вивчення цієї дисципліни безпосередньо спирається на: | На результати вивчення цієї дисципліни безпосередньо спираються: |
| Правознавство | Правове регулювання створення та розробки Стартап проектів в Україні |
|  | Право інформаційних технологій |
|  |  |

**Провідний лектор:**

проф., доц. Перевалова Л.В **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(посада, звання, ПІБ) (підпис)

(посада, звання, ПІБ) (підпис)