# СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

## Захист персональних даних

| | | | |
|---|---|---|---|
| **спеціальність** | **081 «Право»** | **обов'язковість дисципліни** | **вибіркова** |
| **освітня програма** | **081 «Право»** | **факультет** | **Менеджменту, адміністрування та права** |
| **освітній рівень** | **перший (бакалаврський)** | **кафедра** | **Державно-правових дисциплін та міжнародного права** |

## ВИКЛАДАЧ


### Глущенко Світлана Ігорівна

**Вища освіта - спеціальність правознавство**
**Вища освіта – спеціальність економіст-бухгалтер**
**Науковий ступень - кандидат економічних наук 08.00.04 Економіка та управління підприємствами (за видами економічної діяльності)**
**Вчене звання - доцент кафедри державно-правових дисциплін та міжнародного права**
**Практикуючий адвокат**
**Показники професійної активності з тематики курсу:**

- авторка та співавторка тематичних публікацій;
- учасниця наукових і методичних конференцій.

| | | | | | |
|---|---|---|---|---|---|
| **телефон** | **0679291812** | **електронна пошта** | **s_i_glushchenko@ukr.net** | **дистанційна підтримка** | **Google Meet https://meet.google.com/jvt-upgs-yiu** |


## ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

| | |
|---|---|
| **Мета** | **Мета навчальної дисципліни: поглиблення та систематизація знань щодо реалізації законодавства про захист персональних даних, підвищення рівня професіоналізму при реалізації завдань у сфері захисту персональних даних.** |

| | |
|---|---|
| **Формат** | **лекції, практичні заняття, самостійна робота, індивідуальні завдання, командна робота** |
| **Специфічні результати навчання і форми їх контролю** | **У результаті вивчення навчальної дисципліни студент повинен набути такі результати навчання:**<br>**знання:**<br>**- системи нормативно-правових документів, що регулюють суспільні відносини у сфері захисту персональних даних;**<br>**- основних засобів захисту персональних даних, їх організаційних та правових особливостей функціонування;**<br>**- співвідношення між міжнародними та національними засобами захисту персональних даних, можливості застосування міжнародного права при забезпеченні захисту персональних даних;**<br>**- загальних та особливих вимог до обробки персональних даних.**<br>**Уміння:**<br>**- використовувати існуючі правові та організаційні інструменти для захисту персональних даних;**<br>**- проводити базовий аналіз конкретної ситуації для формування власної думки щодо наявності чи відсутності порушення у сфері захисту персональних даних;**<br>**- застосовувати норми та положення законодавства щодо захисту і обробки персональних даних;**<br>**- сприяти захисту основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.**<br>**Навички:**<br>**- уникнення порушень прав людини і громадянина під час обробки та захисту їх персональних даних;**<br>**- оцінювання проблемних ситуацій з позиції гарантування прав суб'єктів персональних даних.**<br>**.** |
| **Обсяг і форми контролю** | **3 кредити ECTS ( 30 годин): 12 годин лекції, 18 годин лабораторно-практичні; модульний контроль (2 модулі);підсумковий контроль – диференційований залік.** |
| **Вимоги викладача** | **вчасне виконання завдань, активність, командна робота** |
| **Умови зарахування** | **згідно з навчальним планом** |

| **ВІДПОВІДНІСТЬ СТАНДАРТУ ОСВІТИ І ОСВІТНІЙ ПРОГРАМІ** | | | |
|---|---|---|---|
| **Компетентеності** | **ЗК1. Навички правової грамотності, що дозволяють оірєнтуватися у світі документованої інформації.**<br>**ЗК5. Визначати правовий статус документів відповідно до їхнього інформаційного змісту.**<br>**ЗК6. Користуватися грифами обмеження доступу до інформації** | **Програмні результати навчання** | **ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень.**<br>**ПРН 9. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на обєктах інформаційної діяльності.**<br>**ПРН-13. Уміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією. ПРН-17. Уміти підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації.**<br>**ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.** |

| | | | |
|---|---|---|---|
| | **при складанні документів, що містять конфіденційну інформацію**<br>**ФКН1. Захищати свої інформаційні права та свободи в умовах їх порушення, втручання у приватне життя, обмеження права на інформацію тощо.** | | **ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.**<br>**ПРН-21. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.**<br>**ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.**<br>**ПРН-24. Уміти здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності.**<br>**ПРН-25. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.**<br>**ПРН-31. Уміти проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.**<br>**ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в IT системах та мережах.** |

**СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)**

| | | | | | |
|---|---|---|---|---|---|
| **модуль 1. Загальні положення підприємницького права** | | | | | |
| **Лекція 1.** | **Персональні данні: понятійний апарат, права та обов'язки усіх заінтересованих сторін** | **Практичне заняття 1 (ПЗ 1)** | **Персональні данні: понятійний апарат, права та обов'язки усіх заінтересованих сторін** | | **Самостійна робота** студентів може включати різні форми, які визначаються робочою навчальною програмою залежно від мети, завдань та змісту дисципліни, зокрема: 1- опрацювання теоретичних основ прослуханого лекційного матеріалу; 2- вивчення окремих тем або питань, що передбачені для самостійного опрацювання; 3- виконання домашніх завдань; 4- підготовка до семінарських (практичних, лабораторних) занять; 5- підготовка до контрольних робіт та інших форм поточного контролю; 6- вирішення і письмове оформлення задач, схем, діаграм, інших робіт |
| **Лекція 2.** | **Вимоги та підстави обробки персональних даних** | **ПЗ 2** | **Вимоги та підстави обробки персональних даних** | | |
| **Лекція 3** | **Суб'єкти обробки персональних даних (володілець, розпорядник). Особливості правовідносин між ними** | **ПЗ 3** | **Суб'єкти обробки персональних даних (володілець, розпорядник). Особливості правовідносин між ними** | | |
| | | | | | |
| **модуль 2. Правове регулювання здійснення підприємницької** | | | | | |
| | | | | **Самості йна** | |
| **Лекція 4.** | **Обробка персональних даних в державних органах та установах різних форм власності. Особливі** | **ПЗ 4** | **Обробка персональних даних в державних органах та установах різних форм власності. Особливі** | | |

| | | | | | |
|---|---|---|---|---|---|
| | **вимоги до обробки чутливих персональних даних** | | **вимоги до обробки чутливих персональних даних** | | графічного характеру; 7- систематика вивченого матеріалу дисципліни перед написанням модулів; 8- відпрацювання завдань тренінгів з дисципліни; 9- аналіз конкретної виробничої ситуації та підготовка аналітичної записки; 10- виконання індивідуальних завдань тощо.<br>**Індивідуальні завдання** є однією з форм самостійної роботи студентів, яка передбачає створення умов для якнайповнішої реалізації творчих можливостей студентів і має на меті поглиблення, узагальнення та закріплення знань, які студенти одержують в процесі навчання, а також застосування цих знань на практиці<br>**До індивідуальних завдань** належать: підготовка рефератів, есе, виконання розрахункових, графічних робіт, оформлення звітів, аналіз практичних ситуацій, підготовка реферативних матеріалів з фахових публікацій, власні дослідження до конференцій, участь в олімпіадах тощо.<br>**Можливі види самостійної роботи студентів та форми контролю** |
| **Лекція 5.** | **Новації, що стануть результатом реформування національного законодавства про захист персональних даних** | **ПЗ 5** | **Новації, що стануть результатом реформування національного законодавства про захист персональних даних** | | |
| **Лекція 6.** | **Запит на доступ до персональних даних. Організаційно-правове забезпечення функціонування системи обробки персональних даних у державному органі** | **ПЗ 6** | **Запит на доступ до персональних даних. Організаційно-правове забезпечення функціонування системи обробки персональних даних у державному органі** | | |

## ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

| | | | |
|---|---|---|---|
| **Література** | 1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII<br>2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР<br>3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII<br>4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-ДСТУ 3396.0-96 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=3 8836.<br>5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. Укази президента: № 685/2021Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».<br>6. Указ президента України №685/2021. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року Постанова Кабінету Міністрів України<br>7. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373<br>8. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1]<br>9. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518. Нормативні документи<br>10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу<br>11. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. https://zakon.rada.gov.ua/rada/show/v0215519-13.<br>12. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id =101798&cat_id-89734&ctime=1344500065981<br>13. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327. 15. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги. 16. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342. | **Методичне забезпечення** | 14. Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2018. 2<br>15. Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2018.– с.776<br>16. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2018. – 432 с.<br>17. Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2018.<br>18. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К: ПолиграфКонсалтинг, 2020. 317 с.<br>19. Пащенко Р.Е. Красношапка І.В. Максюта Д.В. Генерування та формування сигналів. Харків: ХУПС. 2019. 200 с. 25. Хорев А.А. Техническая защита информации/ учеб. пособие для студентов вузов/ в 3-х томах. − т. 1: Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2018. - 436 с. |

# СИСТЕМА ОЦІНЮВАННЯ

| СИСТЕМА | | БАЛИ | ДІЯЛЬНІСТЬ, ЩО ОЦІНЮЄТЬСЯ |
|---|---|---|---|
| **Підсумкове оцінювання** | **100 бальна ECTS (стандартна)** | **до 50** | **50% від усередненої оцінки за модулі** |
| | | **до 50** | **підсумкове тестування** |
| **Модульне оцінювання** | **100 бальна сумарна** | **до 50** | **відповіді на тестові питання** |

| | | | |
|---|---|---|---|
| | | до 20 | усні відповіді на практичних заняттях |
| | | до 30 | результат засвоєння блоку самостійної роботи |

## НОРМИ АКАДЕМІЧНОЇ ЕТИКИ ТА ДОБРОЧЕСНОСТІ

**Всі учасники освітнього процесу (в тому числі здобувачі освіти) повинні дотримуватися кодексу академічної доброчесності та вимог, які прописані у положенні «Про академічну доброчесність учасників освітнього процесу ДБТУ»: виявляти дисциплінованість, вихованість, поважати гідність один одного, проявляти доброзичливість, чесність, відповідальність.**