

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА**

Навчально-науковий юридичний інститут

Кафедра правоохоронної діяльності

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ КІБЕРЗАХИСТУ

Рівень вищої освіти – перший (бакалаврський)

Освітньо-професійна програма «Правоохоронна діяльність»

Спеціальність 262 Правоохоронна діяльність

Галузь знань 26 Цивільна безпека

Затверджено на засіданні кафедри
правоохоронної діяльності
Протокол № 1 від 02.09.2024 р.

м. Івано-Франківськ - 2024

1. Загальна інформація	
Назва дисципліни	Державна політика у сфері кіберзахисту
Викладач	Яцина Максим Олександрович, Гуменицька Валентина Володимирівна
Контактний телефон викладача	0342 59 61 34
Е-mail викладача	maksym.iatsyna@pnu.edu.ua, valentyana.humenytska@pnu.edu.ua
Формат дисципліни	очний
Обсяг дисципліни	3 кредити ЄКТС, 90 годин
Посилання на сайт дистанційного навчання	https://d-learn.pnu.edu.ua/ При вивченні навчальної дисципліни можуть використовуватися можливості платформ Google Classroom, Google Meet, Zoom та ін.
Консультації	Консультації проводяться відповідно до Графіку індивідуальних занять зі студентами, розміщеному на інформаційному стенді та сайті кафедри. Також можливі консультації шляхом листування через корпоративну електронну пошту
2. Анотація до навчальної дисципліни	
<p><u>Предметом</u> вивчення навчальної дисципліни є формування у студентів цілісного розуміння основних принципів, механізмів та інструментів державної політики у сфері кіберзахисту, аналіз національної та міжнародної нормативно-правової бази, вивчення основних кіберзагроз та стратегій протидії їм.</p>	
3. Мета та цілі навчальної дисципліни	
<p><u>Метою</u> вивчення навчальної дисципліни є оволодіння студентами із базовими поняттями і принципами інформаційної безпеки, кібербезпеки та кіберзахисту, а також правовими аспектами забезпечення кібербезпеки та захисту персональних даних в інформаційному просторі.</p> <p>Основними <u>цілями</u> вивчення дисципліни є: оволодіння студентами ключовими поняттями, такими як «кіберзахист», «кібербезпека», «кіберпростір», «кіберзлочинність», «кіберзлочин», «кібертероризм» та ін.; формування навичок здійснення комплексного дослідження нормативно-правової бази кібербезпеки України та міжнародного досвіду у цій сфері, включаючи практичні аспекти; оволодіння методикою оцінки сучасних кіберзагроз; проведення детального аналізу структури, повноважень та функцій суб'єктів національної системи кібербезпеки; формування здатності застосовувати отримані знання на практиці.</p>	
4. Програмні компетентності та результати навчання	
<p><u>Загальні компетентності:</u></p> <ul style="list-style-type: none"> - здатність застосовувати знання у практичних ситуаціях; - здатність використовувати інформаційні та комунікаційні технології; - здатність вчитися і оволодівати сучасними знаннями; - здатність працювати в команді. <p><u>Спеціальні компетентності:</u></p> <ul style="list-style-type: none"> - здатність до критичного мислення та системного аналізу правових явищ; - здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати 	

правову інформацію з різних джерел;

- здатність у межах своєї компетенції забезпечувати законність та правопорядок, безпеку особи та суспільства, протидіяти нелегальній (незаконній) міграції, тероризму та торгівлі людьми, незаконному обігу наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів;

- здатність у межах своєї компетенції ефективно забезпечувати публічну (громадську) безпеку та порядок, у тому числі під час масових правопорушень, запобігати та протидіяти домашньому насильству;

- здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних;

- здатність надавати правоохоронні послуги;

- здатність до аналізу та оцінки причин, умов та факторів, що впливають на вчинення кримінальних та адміністративних правопорушень;

- здатність визначати особу правопорушника, аналізувати кількісні та якісні показники злочинності;

- здатність забезпечувати відповідно до посадових обов'язків охорону об'єктів державної власності, державну охорону органів державної влади України та безпеку взятих під захист осіб, охорону фізичних осіб та об'єктів приватної і комунальної власності;

- здатність застосовувати криміналістичну техніку, оперативно-технічні засоби, у тому числі при проведенні оперативно-розшукових заходів та негласних слідчих (розшукових) дій;

- здатність правомірно застосовувати засоби фізичного впливу, спеціальні засоби та вогнепальну зброю, тактичні прийоми з дотриманням стандартів особистої безпеки, а також надавати невідкладну, зокрема домедичну і медичну допомогу;

- здатність здійснювати контроль за дотриманням фізичними та юридичними особами спеціальних правил та порядку зберігання і використання зброї, спеціальних засобів індивідуального захисту та активної оборони, боєприпасів, вибухових речовин і матеріалів, інших предметів, матеріалів і речовин, на які поширюється дозвільна система;

- здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури;

- здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом;

- здатність вживати заходів з метою запобігання, виявлення та припинення кримінальних та адміністративних правопорушень, усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення правопорушення;

- здатність здійснювати взаємодію з іншими суб'єктами сектору безпеки і оборони, у тому числі при усуненні потенційних та реальних загроз державному суверенітету та територіальній цілісності держави.

Програмні результати навчання:

- виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки;

- застосовувати вогнепальну зброю та спеціальні засоби (штатне та бойове озброєння), фізичну силу; інформаційні системи та технології, технології захисту даних, методи обробки, накопичення та аналізу інформації, інформаційно-аналітичні системи, бази даних (в тому числі міжвідомчі та міжнародні), криміналістичні та оперативно-технічні засоби, безпілотну авіацію, іншу спеціальну та військову техніку і спорядження;

- організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.

5. Організація навчання

Обсяг навчальної дисципліни

лекції	12		
семінарські	18		
практичні	0		
лабораторні	0		
самостійна робота	60		
Ознаки навчальної дисципліни			
Семестр	спеціальність	Курс (рік навчання)	Нормативний / вибірковий
II	262 Правоохоронна діяльність	1-ий	Нормативний
Тематика навчальної дисципліни			
Тема	кількість год.		
	лекції	сем/пр/лаб заняття	сам.роб.
Теоретичні основи інформаційної безпеки, кібербезпеки та кіберзахисту	2	2	7
Правова основа державної політики у сфері кібербезпеки України	2	2	7
Виклики та загрози національній безпеці України у сфері кібербезпеки	2	4	9
Кібертероризм у сучасному світі: поняття, види та шляхи протидії	2	2	7
Організаційно-правові засади забезпечення кібербезпеки України	2	4	9
Юридична відповідальність за кіберзлочини	2	2	7
Особливості нормативно-правового забезпечення кібербезпеки в країнах світу	0	2	7
ЗАГ.:	12	18	60
6. Система оцінювання навчальної дисципліни			
Загальна система оцінювання навчальної дисципліни	Визначається Порядком організації та проведення оцінювання успішності здобувачів вищої освіти Прикарпатського національного університету імені Василя Стефаника, введеним в дію наказом ректора Прикарпатського національного університету імені Василя Стефаника від 19 травня 2023 р. № 309. https://efund.pnu.edu.ua/wp-content/uploads/sites/172/2023/09/poriadok-orhanizatsii-ta-provedennia-otsiniuvannia-		

	<p>uspishnosti-zdobuvachiv-vyshchoi-osvity.pdf , а також Методичними рекомендаціями до порядку оцінювання успішності здобувачів вищої освіти у навчально-науковому юридичному інституті (далі - МРПОУ), затвердженими Вченою радою навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника, протокол №13 від 27 червня 2024 року) https://law.pnu.edu.ua/wp-content/uploads/sites/100/2024/11/metodychni-rekomendatsii-pro-poriadok-otsiniuvannia-uspishnosti.pdf</p>
Вимоги до письмових робіт	<p>Передбачається виконання 1 письмової модульної контрольної роботи (абз.2 пп. 3.1.3.1 МРПОУ). Робота виконується на останньому практичному занятті та охоплює всі теми. Зміст питань, форма та структура завдань визначається викладачами, що проводять практичні заняття за погодженням з керівником навчальної дисципліни та затверджується на засіданні відповідної кафедри (пп. 3.1.3.2 МРПОУ).</p> <p>На письмову модульну контрольну роботу виноситься 1 описове завдання, яке оцінюється в 6 балів, 1 коротке завдання нормативного змісту, яке оцінюється в 6 балів та 8 тестових запитань, кожне з яких оцінюється в 1 бал. Максимальний бал за контрольну становить 50. (пп. 2.6.1 МРПОУ).</p>
Практичні заняття	<p>Завдання для практичних занять визначені у методичних вказівках, що розміщені на сайті кафедри правоохоронної діяльності , а також в системі дистанційного навчання. Максимальна кількість балів за практичні заняття – 45 (пп. 2.6.1–2.6.2 МРПОУ).</p>
Умови допуску до підсумкового контролю	<p>Студенту виставляється залік за умови виконання всіх видів робіт, передбачених навчальною програмою. Наявність хоча б одного пропущеного і невідпрацьованого практичного заняття є підставою для не виставлення заліку (пп. 3.2.2 МРПОУ).</p>
Підсумковий контроль	<p>Залік. Підсумковий бал складається з суми підсумкового балу за практичні заняття (максимально 45 балів), балу за підсумкову модульну контрольну роботу (максимально 50 балів) та балу за самостійну роботу (максимально 5 балів, пп. 2.6.3 МРПОУ). Бал за індивідуальну роботу та/або участь у</p>

науковій роботі (максимально 10 балів) є додатковим балом, який додається до підсумкового семестрового балу (пп. 2.6.1 МРПОУ). Підсумковий бал становить максимально 100 балів (пп. 2.6.1–2.6.3 МРПОУ).

7. Політика навчальної дисципліни

Письмові роботи:

Зміст питань, форма та структура завдань та інструкції щодо виконання обов'язкових (письмової модульної контрольної роботи) та додаткових (письмових завдань за питаннями самостійного опрацювання, письмових експрес-опитувань тощо) письмових робіт визначаються викладачем, що проводить практичні заняття (Розділ 3 МРПОУ). За бажанням (для отримання додаткових балів) студенти можуть виконувати індивідуальні завдання (пп. 3.1.4.1-3.1.4.3 МРПОУ). Види, інструкції щодо виконання індивідуальних завдань знаходяться на кафедрі та на сайті кафедри правоохоронної діяльності (<https://kpd.pnu.edu.ua>).

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, визначених Положенням про запобігання академічному плагіату та іншим порушенням академічної доброчесності у навчальній та науково-дослідній роботі здобувачів освіти Прикарпатського національного університету імені Василя Стефаника <https://pnu.edu.ua/wp-content/uploads/2022/09/Нова-редакція-Положення-про-запобігання-академічному-плагіату.pdf>, усвідомлюючи наслідки порушення.

Реагування на порушення академічної доброчесності здійснюється відповідно до встановлених процедур https://efund.pnu.edu.ua/wp-content/uploads/sites/172/2024/05/pr.01.1.1-08_2024-protsedura_8_universytet.pdf.

Відвідування занять:

Очікується, що всі студенти відвідають всі практичні заняття. Пропуски занять відпрацьовуються в обов'язковому порядку. Студент зобов'язаний відпрацювати пропущене заняття впродовж двох тижнів з дня пропуску заняття (абз. 1. п. 3.1.2 МРПОУ). За пропущені лекційні заняття без поважних причин в обсязі, що перевищує 10% від загальної кількості лекційних годин, які відведені на навчальну дисципліну відповідно до робочого навчального плану, керівник курсу віднімає 5 балів від підсумкового семестрового балу студента (абз. 2. п. 3.1.2 МРПОУ).

Неформальна освіта:

Питання визнання результатів навчання, отриманих у неформальній освіті регулюється Положенням про визнання результатів навчання, здобутих шляхом неформальної освіти, в Прикарпатському національному університеті імені Василя Стефаника https://efund.pnu.edu.ua/wp-content/uploads/sites/172/2023/05/02-07.33_2022-polozhennia-pro-vyznannia-rezultativ-navchannia-zdobutykh-shliakhom-neformalnoi-osvity-v-rykarpatskomu-natsionalnomu-universyteti-imeni-vasylii-stefanyka.pdf

8. Рекомендована література

1. Основи кіберпростору, кібербезпеки та кіберзахисту / В. Богуш та ін. Ліра-К, 2021. 554 с. ISBN 978-617-7844-54-8.

2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
4. Бутузов В.М., Василичук В.І. Протидія комп'ютерній злочинності в Україні: системно-структурний аналіз: монографія. Київ: КНТ, 2021. 408 с.
5. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади : монографія. Одеса : Гельветика, 2020. 486 с.
6. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ : Вид-во “Ліра-К”, 2021. 412 с.
7. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика / С. Петков та ін. ЦУМ, 2022. 460 с. ISBN 978-611-01-2496-6.
8. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор». 2019. 272 с. ISBN 978-617-7729-49-4, URL: https://pdf.lib.vntu.edu.ua/books/2021/Lisovska_2019_272.pdf
9. Філіпова Т. Проблеми протидії кіберзлочинності в Україні. Київ: Генеза, 2020. 280 с.
10. Шевченко О. Вдосконалення кримінального законодавства України у сфері кіберзлочинності. Харків: Основа, 2021. 210 с.

Викладачі: Максим ЯЦИНА
Валентина ГУМЕНИЦЬКА