СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ
ТА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ»

Рівень освіти	другий (магістерський)
Спеціальність	281 Публічне управління та адміністрування
Освітньо-професійна програма	Публічне управління та адміністрування
Тривалість викладання	4-та чверть
Кількість кредитів	4 кредити ЄКТС (120 годин)
Заняття:	
лекції:	2 години на тиждень
практичні:	4 години на тиждень
Мова викладання	Українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5366

Кафедра, що викладає: Державного управління і місцевого самоврядування (ДУМС)

Викладачі:

Баштанник Віталій Володимирович
д.держ.упр., професор, професор кафедри
Персональна сторінка
https://palsg.nmu.org.ua/ua/kafedra/teachers/Bashtannyk/Bashtannyk.php

E-mail: Bashtannyk.V.V@nmu.one

Кравцов Олег Валентинович
к.х.н., доцент кафедри

E-mail: Kravtsov.Ol.V@nmu.one

1. Анотація до курсу

Стрімкий розвиток цифрових технологій та активне впровадження електронних сервісів у державному й приватному секторах зумовлюють безпрецедентне зростання ризиків у сфері інформаційної безпеки. Дисципліна «Правові аспекти захисту інформаційних систем та забезпечення кіберстійкості» висвітлює ключові положення національного та міжнародного законодавства, що регламентують діяльність із захисту даних і гарантують безпечне функціонування інформаційних систем. Увага зосереджується на тому, як законодавчі норми, відповідні стандарти та політики сприяють створенню цілісної системи кіберзахисту, здатної протидіяти сучасним загрозам і забезпечувати належний рівень конфіденційності, цілісності й доступності даних.

У межах дисципліни розглядається комплекс правових механізмів, покликаних не лише запобігти несанкціонованому доступу чи кібератакам, але й встановити процедури реагування на інциденти. Особливу увагу приділено Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних» та пов'язаним нормативним актам. Крім того, вивчаються міжнародні практики та регламенти (наприклад, GDPR), що впливають на вітчизняну правову базу й сприяють гармонізації норм у контексті світових вимог та євроінтеграційних процесів.

Розглядаються питаннях розмежування прав і відповідальності суб'єктів, залучених до захисту інформаційних ресурсів: від власників та операторів до провайдерів хмарних сервісів і державних органів. В умовах активного використання інтернету речей (IoT), штучного інтелекту та великих даних зростає потреба у чіткому регулюванні правових відносин, зокрема захисту прав користувачів і забезпечення мінімізації кібершкідливих впливів. Аналізуються також механізми державного нагляду й контролю, процедурні аспекти розслідування кіберзлочинів і роль міжнародної співпраці в розвитку світової мережі обміну інформацією про кібератаки.

2. Мета та завдання курсу

Мета дисципліни – формування у здобувачів вищої освіти комплексу спеціальних знань щодо правових основ, що визначають сутність, задачі, принципи та сучасні інформаційні технології кібербезпеки, методологічними та законодавчими основами організації, планування та впровадження систем захисту інформації в організаціях, а також основними аспектами практичної діяльності по їх створенню, забезпеченню функціонуванню та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завдання дисципліни:

знати і розуміти:

- законодавчі та нормативно-правові засади захисту інформації та кібербезпеки в Україні, включно з основними вимогами до захисту інформаційних систем;
- міжнародні стандарти й регламенти (GDPR, директиви ЄС тощо), що визначають загальні підходи до безпеки даних та забезпечення кіберстійкості;
- механізми правової відповідальності за порушення у сфері захисту інформації, а також процедури розслідування та судового розгляду кіберінцидентів;
- роль та повноваження державних органів у сфері кібербезпеки, порядок державного нагляду й контролю, а також вимоги до ліцензування та сертифікації діяльності з забезпечення інформаційної безпеки;
- юридичні аспекти розробки й впровадження політик безпеки та процедур реагування на інциденти, включно з вимогами конфіденційності та захисту персональних даних.

вміти:

- аналізувати та інтерпретувати положення законодавчих і нормативно-правових актів у галузі інформаційної та кібербезпеки, визначати обов'язки та межі відповідальності суб'єктів захисту інформації;
- ідентифікувати правові ризики при організації захисту інформаційних систем, розрізняти типи правопорушень у сфері кібербезпеки та давати їм належну кваліфікацію;
- застосовувати національні та міжнародні правові норми й стандарти для планування комплексної системи захисту інформації й кіберстійкості організації;
- розробляти організаційно-розпорядчі документи (політики, регламенти, договори про конфіденційність), що відповідають чинному законодавству та вимогам кібербезпеки;

– оцінювати юридичні аспекти впровадження технічних і процедурних заходів безпеки, зокрема щодо захисту персональних даних, комерційної таємниці та критичної інфраструктури, а також готувати рекомендації щодо усунення виявлених невідповідностей.

3. Результати навчання

Дисциплінарні результати навчання:

– продемонструвати розуміння реальних та потенційних загроз у сфері інформаційної безпеки та нормативно-правових шляхів їх запобігання

– продемонструвати знання основ законодавчої та нормативно нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки

– продемонструвати вміння застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки

– продемонструвати здатність реалізовувати комплексні системи захисту інформації в інформаційних системах (АС) організації відповідно до вимог нормативно нормативно-правових документів

– продемонструвати навички вирішення задач забезпечення та супроводу комплексних систем захисту інформації згідно встановленої політики інформаційної і і\або кібербезпеки

4. Структура курсу

Тижні	Тематика занять	Вид занять	Ресурси	Оцінка
1-2	Вступ до курсу Мета, завдання, результати Політика курсу Навчальні матеріали Система та критерії оцінювання	Лекція	Силабус Презентація курсу Методичні рекомендації Рекомендовані джерела Тест для проведення заліку	–
	Тема 1**. Кібергіростір і кібербезпека: проблеми, перспективи, технології.**		Презентація за темою Рекомендовані джерела	0-2
	Практичне заняття.	Практичне заняття	Методичні рекомендації	0-10
3-4	Тема 2. **Загрози у сфері кібербезпеки**	Лекція	Презентація за темою Рекомендовані джерела	0-2
	Практичне заняття.	Практичне заняття	Методичні рекомендації	0-10
5-6	Тема 3**. Нормативно-правове забезпечення інформаційної та кібербезпеки в Україні**	Лекція	Презентація за темою Рекомендовані джерела	0-2
	Практичне заняття.	Практичне заняття	Методичні рекомендації	0-10
7-8	Тема 4. **Досвід правового забезпечення кібербезпеки у зарубіжних країнах**	Лекція	Презентація за темою Рекомендовані джерела	0-2
	Практичне заняття.	Практичне заняття	Методичні рекомендації	0-10
9-10	Тема 5. **Глобальні аспекти розвитку кіберпростору на основі досвіду протидії кіберзагрозам в умовах російсько-української війни.**	Лекція	Презентація за темою Рекомендовані джерела	0-2

Тижні	Тематика занять	Вид занять	Ресурси	Оцінка
	Практичне заняття.	Практичне заняття	Методичні рекомендації	0-10
	Презентація результатів виконання командного / індивідуального завдання щодо розробки локального нормативного акту про кіберзахист на об'єкті. Підведення підсумків вивчення дисципліни	Практичне заняття	Методичні рекомендації Силабус Тест для проведення заліку	0-40

Індивідуальне завдання «Розробка локального нормативного акту про кіберзахист на об'єкті» полягає у розробленні та захисті здобувачами вищої освіти робочого проекту нормативного акту про кіберзахист на об'єкті.

Форма проведення: розроблення, презентація та захист (відповіді на запитання, дискусія) командного / індивідуального завдання перед аудиторією (бажано використовувати MS PowerPoint).

Для представлення результатів виконання завдання необхідно заповнити відповідний шаблон, який розміщено у застосунку Teams MS Office та на дистанційній платформі Moodle.

Під час презентації і захисту результатів виконання індивідуальних завдань у межах практичних занять передбачено процедуру peer-assessment (оцінювання з боку інших здобувачів освіти).

5. Технічне обладнання та/або програмне забезпечення

Комп'ютерне та мультимедійне обладнання.

Активований корпоративний акаунт НТУ «ДП» (student.i.p@nmu.one).

Microsoft Office 365. Застосунки Microsoft Office: Teams, Forms, Whiteboard, OneNote.

Платформа дистанційного навчання НТУ «ДП» Moodle.

Підключення до Internet.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-59	Незадовільно

Загальні критерії досягнення результатів навчання відповідають описам 7-го кваліфікаційного рівня НРК.

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни **на підставі поточного оцінювання знань** за умови, якщо набрана кількість балів з поточного тестування та виконання і захисту практичних робіт складатиме не менше 60 балів. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Теоретична частина оцінюється за результатами *участі у дискусіях* під час інтерактивних лекцій, виконанню та *презентації результатів індивідуального завдання*, зміст якого описано у розділі 4 (участь у дискусіях та презентація результатів окремих завдань оцінюється в межах 100 балів відповідно до Загальних критеріїв досягнення результатів навчання для 7-го

кваліфікаційного рівня за НРК (магістр)» (див. «Положення про оцінювання результатів навчання здобувачів вищої освіти Національного технічного університету «Дніпровська політехніка» https://cutt.ly/1ORACPD) із подальшим перерахунком відповідно до розподілу балів за окремими темами та завданнями, див. у табл. розділу 4). Загалом за участь у дискусіях і захист результатів виконання індивідуального завдання отримується **максимум 60 балів**.

Практичні роботи (індивідуальні і командні завдання, розподіл балів див. у табл. розділу 4) виконуються під час практичних занять (презентація результатів окремих завдань оцінюється в межах 100 балів відповідно до Загальних критеріїв досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК (магістр)» (див. «Положення про оцінювання результатів навчання здобувачів вищої освіти Національного технічного університету «Дніпровська політехніка» https://cutt.ly/1ORACPD) із подальшим перерахунком відповідно до розподілу балів за окремими темами та завданнями, див. у табл. розділу 4). При несвоєчасному здаванні практичної роботи оцінка знижується вдвічі. У сумі за практичну частину курсу при поточному оцінюванні отримується **максимум 40 балів**.

Отримані бали за теоретичну частину та практичні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Розподіл максимальної кількості балів за складовими поточного контролю:

Теоретична частина	Практична частина	**Разом**
60	40	**100**

6.3. Критерії оцінювання підсумкової роботи. У випадку якщо здобувач вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку проводиться **підсумкове оцінювання (залік)** під час сесії. Якщо здобувач не здав у письмовій формі виконаних індивідуальних завдань (дві практичні роботи), він отримує незадовільну підсумкову оцінку з дисципліни.

Залік проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з **60 тестових завдань і**з чотирма варіантами відповідей, одна правильна відповідь оцінюється в 1 бал **(разом 60 балів)** та **10 тестових завдань** з практичної частини, кожне з запитань оцінюється максимум у 4 бали **(разом 40 балів**), причому:

- 4 бали – відповідність еталону;
- 3 бали – відповідність еталону з незначними помилками;
- 2 бали – часткова відповідність еталону, питання повністю не розкрите;
- 1 бал – невідповідність еталону, але відповідність темі запитання;
- 0 балів – відповідь не наведена або не відноситься до теми запитання.

Отримані бали за відкриті та закриті тести додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 балів.

7. Політика курсу

7.1. Політика щодо академічної доброчесності. Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів) що можуть використовуватися в освітньому процесі. Політика щодо академічної доброчесності

регламентується положенням «Положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка»: http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2. Комунікаційна політика.

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Обов'язком здобувача вищої освіти є перевірка один раз на тиждень (щонеділі) поштової скриньки на НТУ Microsoft Office та відвідування групи дисципліни у Microsoft Teams.

Рекомендуємо створити профілі та підписатися на сторінку кафедри державного управління і місцевого самоврядування у Facebook: https://www.facebook.com/kafedra.publicmanagement/.

Протягом тижнів самостійної роботи обов'язком здобувача вищої освіти є робота у рамках дисципліни дистанційно у застосунку Microsoft Teams та на корпоративній платформі Moodle (www.do.nmu.org.ua).

Усі письмові запитання до викладача стосовно дисципліни мають надсилатися на університетську електронну пошту або до групи у Microsoft Teams.

7.3. Політика щодо перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4. Відвідування занять.

З 24.02.2022 реалізація освітньої діяльності відбувається в умовах правового режиму воєнного стану. Наявна низка небезпек: повітряні тривоги, ризики припинення енергозабезпечення, мобільного та Інтернет-зв'язку. Згідно з наказами по університету у 2024-2025 навчальному році освітня діяльність здобувачів другого (магістерського) рівня вищої освіти всіх форм навчання здійснюється з використанням дистанційних технологій через синхронні та асинхронні комунікації.

Відвідування онлайн лекцій та практичних занять реалізується через приєднання до «наради» в «команді» Microsoft Teams. Під час повітряної тривоги заняття перериваються і продовжуються лише за умов перебування учасників освітнього процесу у захищених приміщеннях. Викладачем (за технічної та безпекової можливості) здійснюється запис заняття для підтримки асинхронного формату навчання.

У випадках відсутності енергозабезпечення, мобільного та Інтернет-зв'язку викладачем забезпечується асинхронний формат навчання та комунікація зі здобувачами за допомогою каналів зв'язку, що функціонують.

Про причини неможливості взяти участь в онлайн заняттях, ускладненні доступу до матеріалів на дистанційних платформах НТУ «ДП» тощо здобувач вищої освіти має повідомити викладача в особистих повідомленнях чатів Microsoft Teams, або листом на корпоративну е-пошту НТУ «ДП», або через старосту чи представника адміністрації інституту.**7.5. Політика щодо оскарження оцінювання**. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може оскаржити виставлену викладачем оцінку у встановленому порядку.

7.6. Зарахування результатів навчання, які отримані у неформальній освіті. Здійснюється відповідно до «Положення про визнання в Національному технічному університеті «Дніпровська політехніка» результатів навчання, набутих у неформальній та/або інформальній освіті» http://surl.li/zopmhq.

7.7. Участь в анкетуванні. Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освіти буде запропоновано анонімно заповнити електронні анкети (MS Forms). Посилання

на форму буде розміщено у Teams курсу. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни.

8. Рекомендовані джерела інформації

Основні

1. Фурашев В., Радзієвська О. «Правове забезпечення інформаційної безпеки : курс лекцій». ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». Київ; Одеса : Фенікс, 2022. -158 с.
2. 2. Вишня Б.В. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с. URL: //er.dduvs.in.ua/bitstream/123456789/4206/1/Основи%20інформаційної%20безпеки%20навчальний%20посібник%2006.2019%20%283%29.pdf
3. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і праваНАПрН України»; Національна бібліотека України ім. В.І. Вернадського. – К., 2021. – № 6 (червень). – 261с - URL: http://ippi.org.ua/sites/default/files/2021-6.pdf
4. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. -URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і праваНАПрН України»; Національна бібліотека України ім. В.І. Вернадського. – К., 2021. – № 5 (травень). – 304с. - URL: http://ippi.org.ua/sites/default/files/2021-5.pdf

Нормативні документи

1. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. // Відом. Верхов. Ради України. – 2011. – № 32. – Ст. 314.
3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007р. // Відом. Верхов. Ради України. – 2007. − № 12. – Ст. 102.
4. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. // Відом. Верхов. Ради України. – 2006. – № 30. – Ст. 258.
5. Про інформаційні агентства: Закон України від 28 лютого 1995 р. // Відом. Верхов. Ради України. – 1995. – № 13. – Ст. 83.
6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. // Відом. Верхов. Ради України. – 1994. – № 31. – Ст. 286.
7. Про науково-технічну інформацію: Закон України від 25 червня 1993 р. // Відом. Верхов. Ради України. – 1993. – № 33. – Ст. 345.
8. 11. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: Закон України від 23 вересня 1997 р. // Відом. Верхов. Ради України. – 1997. – № 49. – Ст. 299; 1998. – № 45. – Ст. 271.
9. 13. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882- IX.

10. 13. Про державну таємницю: Закон України від 21 вересня 1999 р. // Відом. Верхов. Ради України. – 1999. – № 49. – Ст. 428.

11. 14. Про національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191

12. 15. Загальна декларація прав людини, затверджена Генеральною Асамблеєю ООН від 10 грудня 1948 р. URL: http: zakon5.rada.gov. ualawsshow70397%D0

13. 16. Європейська Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: http:zakon5.rada.gov.ua lawsshow 995_004 card4#History

14. 17. Про публічні електронні реєстри : Закон України від 18.11.2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907- 20#Text

15. 18. Про національну безпеку України: Закон України. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

16. 19. Про Стратегію національної безпеки України: Указ президента України №392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

Додаткові

1. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології. /Арістова І.В., Баранов О.А., Дзьобань О.П. та ін.; за заг. ред. проф. К.І. Бєлякова: монографія. Київ: КВІЦ, 2019. 344 с. (Розділ4. Характеристика галузевих видів юридичної відповідальності за інформаційні делікти.) - URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

2. В. П. Горбулін, О. Г. Додонов , Д.В. Ланде. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с. - URL: http://dwl.kiev.ua/art/gdl/gdl.pdf

3. О. Д. Довгань, І. М. Доронін. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О.Д. Довгань, І.М. Доронін; НАПрН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107 с. - URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf

Інформаційні ресурси

1. https://cip.gov.ua/ua
2. https://cert.gov.ua/
3. https://scpc.gov.ua/uk
4. http://www.ligazakon.ua/ Головний правовий портал України
5. https://www.infosecurity-magazine.com/