Силабус освітнього компонента
Програма навчальної дисципліни

Правове регулювання інформаційної безпеки

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
3

Мова викладання
Українська, англійська

Викладачі, розробники

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор понад 170 наукових і навчально-методичних праць (за даними Google Scholar, h-індекс – 12), у тому числі 3 монографій та навчального посібника з грифом.
Має у своєму доробку 10 патентів та 10 авторських свідоцтв.
Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки», «Авторське право у цифровому суспільстві».
Сфера наукових інтересів охоплює питання інтелектуальної власності, правового регулювання кіберпростору, інформаційної безпеки, криптографічних методів захисту, цифрові активи.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна «Правове регулювання інформаційної безпеки» є вибірковим освітнім компонентом, спрямованим на підготовку фахівців у сфері кібербезпеки та інформаційних технологій. Курс охоплює правові основи інформаційного суспільства, правовий режим інформації, захист персональних даних, регулювання діяльності медіа та цифрових платформ, інформацію з обмеженим доступом, відповідальність за порушення в інформаційній сфері та особливості

протидії кіберзлочинам. Особливий акцент зроблено на міжнародних і національних стандартах кіберзахисту, а також на правовому регулюванні цифрових активів (криптовалют, токенів, NFT) та механізмах їх кіберзахисту.

Мета та цілі дисципліни

Мета дисципліни – формування у студентів знань і практичних навичок щодо правового регулювання інформаційної безпеки, захисту інформації та цифрових активів у кіберпросторі, а також умінь застосовувати правові та технічні механізми для запобігання й розслідування кіберінцидентів.

Основні завдання вивчення дисципліни:

засвоєння теоретичних основ інформаційного права та їхнього застосування у сфері кібербезпеки;

набуття знань про міжнародні та національні стандарти кіберзахисту, регулювання персональних даних і цифрового контенту;

вивчення правового режиму інформації з обмеженим доступом та механізмів її захисту;

ознайомлення з правовими аспектами функціонування медіа, цифрових платформ і глобальних інформаційних сервісів;

формування навичок ідентифікації, документування та правової кваліфікації кіберзлочинів, застосування методів цифрової криміналістики;

опанування правових основ регулювання та захисту цифрових активів (криптовалют, токенів, NFT) у національному та міжнародному праві.

Предмет дисципліни – правові норми, інститути та механізми регулювання відносин у сфері інформаційної безпеки, кіберзахисту та цифрових активів, а також методи правового реагування на загрози й порушення у кіберпросторі.

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Результати навчання

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., практичні заняття – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисципліни «Правознавство» – розуміння основних принципів права, системи законодавства та правозастосування;
«Інтелектуальна власність» – знання про правовий режим об'єктів інтелектуальної власності та навички аналізу правових відносин у цифровому середовищі;
«Основи кібербезпеки» (базовий курс) – початкові уявлення про інформаційні загрози, засоби їх виявлення і запобігання.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи. використання онлайн-ресурсів (WIPO, GDPR portal, реєстри судових рішень.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Інформаційне право та кібербезпека. Інформація як об'єкт правового регулювання. Роль права у системі національної кібербезпеки. Закон України " про основні засади забезпечення кібербезпеки"	2
Тема 2. Інформаційне суспільство і сучасні виклики безпеки Інформаційна культура і цифрова грамотність. Кіберзагрози для особи, суспільства, держави. NIST Cybersecurity Framework як модель реагування.	2
Тема 3. Правовий режим інформації та персональних даних. Персональні дані, GDPR та українське законодавство. Конвенції. Витоки даних, кейси кіберінцидентів.	2
Тема 4. Інформаційна діяльність та цифрові сервіси. Е-урядування, реєстри, хмарні сервіси. Захист даних у державних і корпоративних системах. ISO/IEC 27018 як основа для хмарної безпеки	2
Тема 5. Медіа, цифрові платформи та інформаційні війни. Закон «Про медіа», регулювання соцмереж. Маніпуляції, дезінформація, ІПСО. Digital Services Act (ЄС) та досвід України.	2

Тема 6. . Інформація з обмеженим доступом та кіберзахист. Класифікація: державна таємниця, службова, комерційна. Міжнародні стандарти захисту (ISO/IEC 15408). Кіберзахист критичної інфраструктури.	2
Тема 7. Відповідальність за правопорушення та кіберзлочини. Адміністративна і кримінальна відповідальність. Статті ККУ 361–363 (несанкціонований доступ, втручання). Будапештська конвенція про кіберзлочинність. Цифрова криміналістика: збирання доказів	2
Тема 8. Правове регулювання та захист цифрових активів. Криптовалюти, токени, NFT як нові об'єкти права. Закон України «Про віртуальні активи» (2022). Міжнародний досвід (MiCA – ЄС, FinCEN – США). Ризики: відмивання коштів, шахрайство, кіберкрадіжки. Захист цифрових активів: технічні й правові механізми (смарт-контракти, KYC/AML, багаторівневий захист гаманців).	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Місце інформаційного права у системі права України. Поняття та предмет інформаційного права. Зв'язок із конституційним, цивільним, адміністративним та кримінальним правом. Нормативно-правова база (Конституція України, ЦКУ, ККУ, Закон «Про інформацію», Закон «Про доступ до публічної інформації»). Складання схеми «Місце інформаційного права у системі права України». Висновки про інтегративний характер інформаційного права.	4	1
Тема 2. Виявлення та аналіз кіберзагроз для інформаційного суспільства. Основні типи кіберзагроз: фейки, маніпуляції, пропаганда, інформаційні атаки. Ознаки недостовірної інформації у ЗМІ та соцмережах. Інструменти фактчекінгу: StopFake, EU vs Disinfo, Bellingcat, Google Fact Check, InVID. Практичне завдання: обрати 2–3 приклади (новина, пост, стаття), визначити ознаки фейку чи маніпуляції, перевірити достовірність за допомогою інструментів, скласти таблицю з результатами. Висновки про роль фактчекінгу в системі кібербезпеки.	4	1
Тема 3. Авторське право у цифровому середовищі. Авторське право на програмне забезпечення, бази даних, цифровий контент. Порушення авторських прав у мережевому середовищі: піратство, нелегальне копіювання, хакерські витоки. Роль цифрових платформ у забезпеченні захисту авторських прав. Аналіз процедур notice-and-takedown на прикладі YouTube, Facebook, TikTok.	4	1
Тема 4. Персональні дані як об'єкт кіберзахисту. Правовий режим персональних даних за законодавством України. Вимоги GDPR як міжнародного стандарту. Інструменти і методи кіберзахисту персональних даних. Практичне дослідження кейсів витоку даних (наприклад, «Дія», LinkedIn). Висновки щодо відповідальності за порушення режиму персональних даних.	4	1
Тема 5. Цифрові докази та судова експертиза. Огляд ISO/IEC 27001, NIST Cybersecurity Framework, GDPR,	4	1

Будапештської конвенції про кіберзлочинність. Порівняння підходів України та ЄС. Практичне завдання: скласти схему застосування стандарту NIST або ISO/IEC для організації безпеки даних в умовній компанії.		
Тема 6. . Міжнародні стандарти інформаційної безпеки. Методи поширення дезінформації. Вплив інформаційних операцій на суспільство та державу. Інструменти протидії: фактчекінг, кібергігієна, цифрова грамотність. Практичне дослідження прикладів російських інформаційних атак проти України.	4	1
Тема 7. Інформаційні війни та дезінформація. Методи поширення дезінформації. Вплив інформаційних операцій на суспільство та державу. Інструменти протидії: фактчекінг, кібергігієна, цифрова грамотність. Практичне дослідження прикладів російських інформаційних атак проти України.	4	1
Тема 8. Правове регулювання та захист цифрових активів. Криптовалюти, токени, NFT як нові об'єкти права. Закон України «Про віртуальні активи» (2022). Міжнародний досвід (MiCA – ЄС, FinCEN – США). Ризики: відмивання коштів, шахрайство, кіберкрадіжки. Захист цифрових активів: технічні й правові механізми (смарт-контракти, KYC/AML, багаторівневий захист гаманців). Практичне завдання: аналіз кейсів шахрайства з криптовалютами.	4	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Базові принципи побудови та функціонування комп'ютерних мереж. Основні положення теорії взаємодії відкритих систем. Модель OSI та TCP/IP: принципи, рівні, функції. Методи комутації та повторної передачі даних. Мережа Ethernet: розвиток стандартів, особливості роботи, протокол CSMA/CD. Протокол IP (IPv4/IPv6): структура, принципи адресації та маршрутизації.	0,5
Тема 2. Сучасні протоколи, технології та безпека комп'ютерних мереж. Протоколи транспортного рівня: TCP, UDP, RTP, їх застосування. Протоколи маршрутизації: RIP, OSPF (порівняльний аналіз). Сучасні мережеві технології: VPN, хмарні сервіси, SDN. Основи мережевої безпеки: типи атак та методи захисту. Базова конфігурація комутаторів та маршрутизаторів (Cisco Packet Tracer).	0,5
Тема 3. Безпека комп'ютерних мереж та методи її забезпечення. Класифікація загроз у локальних та глобальних мережах. Основні принципи побудови захищених мереж. Методи аутентифікації та шифрування даних. Використання VPN для захисту інформаційних каналів. Фаєрволи, IDS/IPS системи та їх роль у безпеці.	1
Загалом	$\sum_{i=1}^{m} b_i = 2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Національне законодавство у сфері кібербезпеки України. Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Закон України «Про захист персональних даних».	11
Тема 2. Правове регулювання захисту інформації в інформаційно-телекомунікаційних системах. Правові основи державної таємниці та захисту службової інформації, нормативні акти Держспецзв'язку та НБУ у сфері кіберзахисту.	11
Тема 3. Міжнародні стандарти кібербезпеки. ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework (CSF), директиви NIS та NIS2 ЄС.	10
Тема 4. Європейське регулювання у сфері кібербезпеки та даних. Загальний регламент захисту даних (GDPR), директива ЄС про кіберзлочини та кібербезпеку, NIS2 Directive.	10
Тема 5. Міжнародно-правові акти у сфері кібербезпеки. Будапештська конвенція про кіберзлочинність (2001), резолюції та рекомендації ООН у сфері інформаційної безпеки, практика НАТО у сфері кібероборони.	10
Тема 6. Кіберзлочинність і кримінально-правові механізми протидії. Кримінальний кодекс України (розділ XVI), класифікація кіберзлочинів за INTERPOL та EUROPOL.	10
Тема 7. Захист прав людини в кіберпросторі. Право на приватність у цифрову епоху, Європейська конвенція з прав людини (ст. 8 – право на повагу до приватного життя), баланс між свободою слова та боротьбою з кіберзлочинністю.	10
Тема 8. Правове регулювання критичної інфраструктури. Поняття та категорії критичної інформаційної інфраструктури, регламенти щодо захисту енергетичних, транспортних та фінансових систем.	10
Тема 9. Етичні та правові аспекти використання технологій штучного інтелекту та Big Data у сфері кібербезпеки. Використання ШІ та Big Data у кіберзахисті створює нові можливості, але породжує правові й етичні виклики: прозорість алгоритмів, відповідальність за їхні рішення, ризики дискримінації та порушення приватності. Значну роль відіграють міжнародні стандарти та регламенти, зокрема GDPR і Європейський акт про ШІ.	10
Тема 10. Практика судів України та ЄС у справах, пов'язаних із кіберзлочинами та кіберзахистом. Судова практика демонструє застосування норм щодо кіберзлочинів і захисту даних. В Україні це справи про несанкціонований доступ і незаконне використання персональних даних, у ЄС – рішення Digital Rights Ireland, Schrems I та II, які визначають підходи до балансу між кібербезпекою та правами людини.	10
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. Курс «Кібергігієна для громадян та організацій» (CERT-UA, Державна служба спеціального зв'язку та захисту інформації України).
https://cybereducation.org.ua
2. Курс «Захист персональних даних: законодавчі вимоги та практичні аспекти» (Prometheus).
https://prometheus.org.ua
3. Курс «Кібербезпека та право» (Вища школа адвокатури НААУ).
https://hsa.org.ua
4. «Cybersecurity Law and Policy» (Harvard Online, edX).
https://online-learning.harvard.edu/course/cybersecurity-law-and-policy
5. «EU Cybersecurity and Data Protection Regulation» (Coursera, Leiden University).
https://www.coursera.org/learn/cyber-security-european-union
6. «NIS2 Directive and EU Cybersecurity Compliance» (FutureLearn).
https://www.futurelearn.com/courses/nis2-directive
7. «Data Protection and Privacy Law (GDPR)» (Udemy).
https://www.udemy.com/course/general-data-protection-regulation/
8. «Cybercrime Law and the Budapest Convention» (Council of Europe Training Platform).
https://www.coe.int/en/web/cybercrime/octopus-online-interactive-tools

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Правове забезпечення інформаційної безпеки: навчальний посібник / В. П. Горбулін, О. Г. Баранов, В. Ю. Цимбалюк. – К. : НАУ, 2015. – 368 с.
http://elar.naiau.kiev.ua/jspui/bitstream/123456789/4852/1/Pravove_zabezpechennia_informatsiinoi_bezpeky.pdf
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII.
https://zakon.rada.gov.ua/laws/show/2163-19
3. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII (із змінами).
https://zakon.rada.gov.ua/laws/show/2657-12
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР.
https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
5. Directive (EU) 2016/1148 (NIS Directive) concerning measures for a high common level of security of network and information systems across the Union.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
6. Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). – Brussels, 2020.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0823
7. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.
https://www.iso.org/standard/82875.html
8. NIST Cybersecurity Framework (CSF). – National Institute of Standards and Technology (USA), 2018.
https://www.nist.gov/cyberframework

9. NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg: NIST, 2020.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
10. Кібербезпека та кіберзахист: навчальний посібник / С. Є. Остапов, С. П. Євсєєв, О. Г. Король. – К. : НАУ, 2021. – 482 с.
http://kist.ntu.edu.ua/textPhD/kiberbezpeka.pdf
11. Романчук О. Ю. Правове регулювання кіберзлочинності в Україні: монографія. – Львів : ЛНУ імені Івана Франка, 2020. – 298 с.
https://dspace.lnu.edu.ua/bitstream/123456789/36589/1/Romanchuk.pdf
12. Budapest Convention on Cybercrime (2001). Council of Europe.
https://www.coe.int/en/web/cybercrime/the-budapest-convention

Додаткова література

8. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,6	0,4		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A

знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Сергій ЄВСЕЄВ