Заклад вищої освіти
«Міжнародний науково-технічний університет
імені академіка Юрія Бугая»

Кафедра права

ПРАВОВЕ РЕГУЛЮВАННЯ ОСНОВ КІБЕРБЕЗПЕКИ

Силабус навчальної дисципліни

на 2021/2022 навчальний рік

Реквізити навчальної дисципліни	
Рівень вищої освіти	Другий (магістерський)
Галузь знань	12 «Інформаційні технології»
Статус дисципліни	Вибіркова
Форма навчання	Денна
Рік підготовки, семестр	І курс, 2 семестр
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	4 кредити/120 годин
Семестровий контроль/ контрольні заходи	Модульний контроль
Мова викладання	Українська
Формат навчальної дисципліни	Змішаний (blended)
Викладач 	**ДЕРКАЧЕНКО ЮЛІЯ ВІКТОРІВНА** **Посада:** доцент кафедри права **Науковий ступінь:** кандидат юридичних наук **Вчене звання:** - **Профайл викладача:** https://scholar.google.com.ua/citations?user=APxJmDsAAAAJ&hl=uk **ORCID:** https://orcid.org/0000-0002-3019-9730 **Телефон:** +380955554110 **E-mail:** j.derkachenko@istu.edu.ua
Розміщення курсу	**Код курсу Google classroom:** https://classroom.google.com/c/MzE5NjM2NTc2MDE1?cjc=lmzfrek **Посилання Meet:** https://meet.google.com/lookup/gr67q2csem

Програма навчальної дисципліни

1. Опис навчальної дисципліни

Метою навчальної дисципліни «Правове регулювання основ кібербезпеки» є формування у майбутніх спеціалістів різних спеціальностей умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, правового регулювання стану та принципів забезпечення кібербезпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій. Вивчення курсу «Правове регулювання основ кібербезпеки» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Правознавство», «Інтелектуальна власність», «Системи інформаційної безпеки»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

Предмет вивчення навчальної дисципліни: сучасні методи та засоби правового регулювання основ кібербезпеки.

Результати навчання за дисципліною (РН):

РН 1. Вміти обстежувати об'єкти та процеси у предметних галузях дослідження (комп'ютеризації), здійснювати їх аналіз.

РН 2. Вміти вибирати та формулювати проблему дослідження, шукати необхідну наукову інформацію, обирати методологічну основу дослідження, реферувати літературні джерела.

РН 3. Вміти формулювати об'єкт і предмет дослідження, формулювати і перевіряти наукові гіпотези, формувати комплекс методик для дослідження обраного предмету.

РН 4. Вміти збирати емпіричні дані, проводити обробку та інтерпретацію емпіричних даних.

РН 5. Вміти оформлювати наукові звіти, представляти результат дослідження на наукових конференціях та семінарах.

РН 6. Вміти аналізувати наукові статті та патенти, знаходити (виявляти) невирішені проблеми, розробляти особисті статті та інші наукові матеріали, планувати наукові дослідження.

2. Пререквізити та постреквізити

Пререквізити: базові знання в галузі інформаційних технологій.

Постреквізити: «Криптографічні методи захисту інформації в ІС», «Мережева безпека», «Системи інформаційної безпеки», «Переддипломна практика», «Дипломне проектування».

3. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. СУТНІСТЬ КІБЕРБЕЗПЕКИ.

Тема 1. Історія розвитку та юридичний аналіз основних понять в сфері кібербезпеки

Тема 2. Види загроз та способи захисту інформації.

Тема 3. Міжнародні стандарти та правові акти в цій галузі.

Тема 4. Міжнародне співробітництво в сфері кібербезпеки.

Тема 5. Кібербезпека і захист прав людини.

ЗМІСТОВИЙ МОДУЛЬ 2. ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Тема 6. Правове регулювання кібербезпеки в Україні.

Тема 7. Об’єкти та суб'єкти кібербезпеки та їх повноваження в Україні.

Тема 8. Департамент кібербезпеки в України та Кіберполіція: основні задачі та функції.

Тема 9. Взаємодія державних органів та приватних компаній у сфері кібербезпеки.

Тема 10. Відповідальність за порушення законодавства з кібербезпеки.

4. Навчальні матеріали та ресурси

Законодавство:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
5. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373 // https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text
6. 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]
7. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
8. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
9. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
12. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
13. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
14. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
15. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
16. Автоматизированные системы. Требования к содержанию документов РД 50-34.698

17. Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89
18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу
19. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)
20. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

Навчальна та наукова література:

1. Словник термінів з кібербезпеки [Текст] / Рада нац. безпеки і оборони України, Міжвідом. н.-д. центр з пробл. орг. злочинності, Нац. акад. СБУ, Навч.-наук. ін-т інформ. безпеки ; [уклад.: Бутузов В. М. та ін. ; за заг. ред. Копана О. В., Скулиша Є. Д.]. - К. : ВБ "Аванпост-Прим", 2012. - 214 с. - ISBN 978-617-502-033-3
2. Кібербезпека мереж наступного покоління [Текст] : навч. посіб. у галузі знань 1701 "Інформаційна безпека" за спец. 8.17010201 - Системи технічного захисту інформації, автоматизація її обробки / О. О. Вараксін [та ін.] ; за ред. чл.-кор. МАЗ В. Г. Кононовича ; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. - О. : ОНАЗ ім. О. С. Попова, 2013. - 238 с. : рис., табл. - Бібліогр.: с. 236-238. - 300 прим. - ISBN 978-617-582-006-3
3. Міжнародні стандарти з кібербезпеки та їх застосування в Україні [Текст] : матеріали "круглого столу" (м. Харків, 19 квіт. 2016 р.) / Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. кримінології та кримін.-викон. права ; за ред. А. П. Гетьмана, Б. М. Головкіна. - Харків : Право, 2016. - 87 с. - Бібліогр. в кінці ст. - 42 прим. - ISBN 978-966-937-024-2
4. Державне управління у сфері забезпечення кібербезпеки України [Текст] : автореф. дис. ... канд. наук з держ. упр. : 25.00.01 / Лук'янчук Руслан Валерійович ; Ін-т законодавства Верхов. Ради України. - Київ, 2017. - 19 с.
5. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення [Текст] : матеріали міжнар. наук.-практ. конф. 21 квіт. 2017 р. : [у 2 ч.] / [упоряд.: В. М. Фурашев. С. Ю. Петряєв] ; НДІ інформатики і права Нац. акад. прав. наук України, Ф-т соціології і права Нац. техн. ун-ту України "Київ .політехн. ін-т ім. Ігоря Сікорського", Ф-т права і адміністрації Варшав. ун-ту. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2017. Ч. 1. - 2017. - 144 с. - Бібліогр. в кінці ст. - 100 прим. - ISBN 978-966-622-833-1
6. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення [Текст] : матеріали міжнар. наук.-практ. конф. 21 квіт. 2017 р. : [у 2 ч.] / [упоряд.: В. М. Фурашев. С. Ю. Петряєв] ; НДІ інформатики і права Нац. акад. прав. наук України, Ф-т соціології і права Нац. техн. ун-ту України "Київ .політехн. ін-т ім. Ігоря Сікорського", Ф-т права і адміністрації Варшав. ун-ту. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2017. Ч. 2. - 2017. - 123 с. - Назва обкл. : Кібербезпека та інтелектуальна власність: проблеми правового забезпечення. Студентський погляд. - Бібліогр. в кінці ст. - 100 прим. - ISBN 978-966-622-834-8
7. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення [Текст] : монографія / І. В. Діордіца ; Запоріз. нац. ун-т. - Запоріжжя : Гельветика, 2017. - 547 с. : табл. - Бібліогр.: с. 476-546. - 300 прим. - ISBN 978-966-916-500-8
8. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України [Текст] : аналіт. доп. / [Д. В. Дубов та ін. ; за заг. ред. Д.

Дубова] ; Нац. ін-т стратег. дослідж. - Київ : НІСД, 2018. - 81 с. - Бібліогр. в знесках. - 150 прим. - ISBN 978-966-554-296-7
9. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки [Текст]. - На заміну ДСТУ ISO/IEC 27032:2015 ; Чинний від 2018-01-01. - Київ : УкрНДНЦ, 2018. - VI, 44 с. : рис., табл. - (Національний стандарт України). - Бібліогр.: с. 43.
10. Засоби та системи технічного захисту інформації [Текст] : навч. посіб. для студентів спец. 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / [І. Є. Антіпов та ін.] ; Харків. нац. ун-т радіоелектроніки. - Харків : Панов, 2018. - 215 с. : рис., табл. - Бібліогр.: с. 202-212. - 300 прим. - ISBN 978-617-7722-26-6
11. Засоби та системи технічного захисту інформації [Текст] : навч. посіб. для студентів спец. 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / [І. Є. Антіпов та ін.] ; Харків. нац. ун-т радіоелектроніки. - Харків : ХНУРЕ, 2019. - 215 с. : рис., табл. - Бібліогр.: с. 202-212. - 100 прим. - ISBN 978-966-659-252-4
12. Основи кібербезпеки та кібероборони [Текст] : підручник / Даник Ю. Г., Воробієнко П. П., Чернега В. М. ; Одес. нац. акад. зв'язку ім. О. С. Попова. - Одеса : ОНАЗ ім. О. С. Попова, 2018. - 227 с. : рис., табл. - Бібліогр.: с. 225-226. - 300 прим. - ISBN 978-617-582-064-3
13. Адміністративно-правові засади забезпечення кібербезпеки України [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.07 / Бухарєв Владислав Вікторович ; Сум. держ. ун-т. - Суми, 2018. - 20 с.
14. Біленчук П. Д. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення [Електронний ресурс] / П. Д. Біленчук, М. І. Малій, Н. І. Сватюк, О. І. Симканич // Юридичний вісник. Повітряне і космічне право. - 2020. - № 4. - С. 156-162. - Режим доступу: http://nbuv.gov.ua/UJRN/Npnau_2020_4_24
15. Грубінко А. В. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти [Електронний ресурс] / А. В. Грубінко // Актуальні проблеми правознавства. - 2021. - Вип. 1. - С. 5-10. - Режим доступу: http://nbuv.gov.ua/UJRN/aprpr_2021_1_3
16. Демедюк С. В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні [Електронний ресурс] / С. В. Демедюк // Південноукраїнський правничий часопис. - 2015. - № 3. - С. 119-123. - Режим доступу: http://nbuv.gov.ua/UJRN/Pupch_2015_3_39
17. Коваленко Н. В. Про правовий режим кібербезпеки в Україні [Електронний ресурс] / Н. В. Коваленко // Актуальні проблеми вітчизняної юриспруденції. - 2016. - Вип. 3. - С. 96-100. - Режим доступу: http://nbuv.gov.ua/UJRN/apvu_2016_3_24
18. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки [Електронний ресурс] / С. В. Демедюк // Південноукраїнський правничий часопис. - 2015. - № 2. - С. 144-147. - Режим доступу: http://nbuv.gov.ua/UJRN/Pupch_2015_2_44
19. Ясенчук Ю. Нормативно-правове регулювання та соціально-психологічний аспект кібербезпеки [Електронний ресурс] / Ю. Ясенчук // Наукові записки з української історії. - 2016. - Вип. 39. - С. 70-73. - Режим доступу: http://nbuv.gov.ua/UJRN/Nzzui_2016_39_12

20. Харченко В. П. Мультирівнева модель даних для ідентифікації забезпеченості вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації [Електронний ресурс] / В. П. Харченко, О. Г. Корченко, С. О. Гнатюк // Захист інформації. - 2017. - Т. 19, № 1. - С. 95-104. - Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2017_19_1_14
21. Акульшина В. Кібербезпека Фінляндії: правовий та інституційний механізми [Електронний ресурс] / В. Акульшина // Медіафорум: аналітика, прогнози, інформаційний менеджмент. - 2017. - Вип.. - С. 158-165. - Режим доступу: http://nbuv.gov.ua/UJRN/mfapim_2017_5_17
22. Жиляєв І. Б. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи [Електронний ресурс] / І. Б. Жиляєв, А. І. Семенченко // Стратегічні пріоритети. - 2017. - № 4. - С. 55-63. - Режим доступу: http://nbuv.gov.ua/UJRN/spa_2017_4_8
Діордіца І. В. Репрезентація термінології кібербезпекової політики в текстах нормативно-правових актів України [Електронний ресурс] / І. В. Діордіца // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2017. - Вип. 29(1). - С. 64-67. - Режим доступу: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_29(1)__18
23. Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави [Електронний ресурс] / І. М. Доронін // Інформація і право. - 2017. - № 1. - С. 104-111. - Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2017_1_13
24. Шуст Н. Б. Теоретико-правові питання кібербезпеки у сфері Інтернету та її стану в Україні, способи захисту від кіберзлочинів [Електронний ресурс] / Н. Б. Шуст, Т. С. Ярошенко, А. В. Яценко // Прикарпатський юридичний вісник. - 2017. - Вип. 5. - С. 110-113. - Режим доступу: http://nbuv.gov.ua/UJRN/Pjuv_2017_5_28
25. Бухарєв В. В. Поняття та особливості кібербезпеки як об'єкта адміністративно-правової охорони [Електронний ресурс] / В. В. Бухарєв // Європейські перспективи. - 2018. - № 3. - С. 11-16. - Режим доступу: http://nbuv.gov.ua/UJRN/evpe_2018_3_4
26. Ткачук Н. А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки [Електронний ресурс] / Н. А. Ткачук // Інформація і право. - 2018. - № 4. - С. 104-111. - Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2018_4_12
27. Сачук Ю. Нормативно-правові засади забезпечення професійної підготовки фахівців із кібербезпеки та захисту інформації [Електронний ресурс] / Ю. Сачук // Молодь і ринок. - 2018. - № 12. - С. 45-50. - Режим доступу: http://nbuv.gov.ua/UJRN/Mir_2018_12_9
28. Бойко В. О. Європейський досвід державно-приватного партнерства у сфері кібербезпеки: підходи до формування нормативно-правових засад [Електронний ресурс] / В. О. Бойко // Стратегічні пріоритети. - 2019. - № 1. - С. 28-36. - Режим доступу: http://nbuv.gov.ua/UJRN/spa_2019_1_5
29. Басараб О. Щодо визначення поняття "кібербезпека Державної прикордонної служби України" – теоретико-правовий аспект [Електронний ресурс] / О. Басараб, О. Басараб, І. Ларіонова. // Вісник Національної академії Державної прикордонної служби України. Серія : Юридичні науки. - 2019. - Вип. 3. - Режим доступу: http://nbuv.gov.ua/UJRN/vnadpcurn_2019_3_5
30. Стець В. Теоретико-правові проблеми визначення сутності кібербезпеки як складової інформаційної безпеки [Електронний ресурс] / В. Стець // Актуальні

проблеми державного управління. - 2019. - Вип. 4. - С. 24-28. - Режим доступу: http://nbuv.gov.ua/UJRN/apdyo_2019_4_6
31. Мялковський Д. В. Організаційно-правові механізми державного управління міжнародним співробітництвом України у сфері кібербезпеки [Електронний ресурс] / Д. В. Мялковський // Теорія та практика державного управління. - 2019. - Вип. 3. - С. 216-226. - Режим доступу: http://nbuv.gov.ua/UJRN/Tpdu_2019_3_28
32. Семенченко А. І. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку [Електронний ресурс] / А. І. Семенченко, В. Л. Плескач, О. А. Заярний, М. В. Плескач // Проблеми програмування. - 2020. - № 2-3. - С. 278-286.
33. Шпачук В. В. Державне управління кібербезпекою України: правовий аспект [Електронний ресурс] / В. В. Шпачук. // Державне управління: удосконалення та розвиток. - 2018. - № 11. - Режим доступу: http://nbuv.gov.ua/UJRN/Duur_2018_11_6
34. Філінович В. В. Кібербезпека та Інтернет речей: правовий аспект [Електронний ресурс] / В. В. Філінович // Юридичний вісник. Повітряне і космічне право. - 2020. - № 4. - С. 122-127. - Режим доступу: http://nbuv.gov.ua/UJRN/Npnau_2020_4_19

Інформаційні ресурси:

Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/.

Навчальний контент

5. Методика опанування навчальної дисципліни

№ тижня	Тема	Заняття	Результат навчання	Контрольний захід
ЗМІСТОВНИЙ МОДУЛЬ №1. СУТНІСТЬ КІБЕРБЕЗПЕКИ				
3	**Т №1.** Історія розвитку та юридичний аналіз основних понять в сфері кібербезпеки	**Л №1.** Розвиток кібербезпеки в Україні та зарубіжних країнах. Дослідження поняття кібербезпека.	РН №№ 1-2	МК №1
3	**Т №2.** Види загроз та способи захисту інформації	**Л №2.** Підходи до побудови національних правових систем захисту персональних даних. Реальні та потенційні загрози в кіберзахисті.	РН № 2	МК №1
4		**ПЗ №2.** Дослідження загроз та способів захисту інформації	РН № 2	МК №1
5	**Т №3.** Міжнародні стандарти та правові акти в цій галузі	**Л №3.** Міжнародно-правове регулювання кібербезпеки	РН № 2	МК №1
6		**ПЗ №3.** Дослідження та вивчення досвіду інших країн із забезпечення кібербезпеки на основі міжнародних стандартів з кібербезпеки	РН № 2	МК №1
5	**Т №4.** Міжнародне співробітництво в сфері кібербезпеки	**Л №4.** Міжнародне співробітництво в сфері кібербезпеки	РН № 2	МК №1
7		**ПЗ №4.** Дослідження можливостей сучасного антивірусного	РН № 2	МК №1

		програмного забезпечення		
7	**Т №5.** Кібербезпека і захист прав людини	**Л №5.** Права і свободи людини, громадянина та їх обов'язки в сфері кібербезпеки	РН № 3	МК №1
8		**ПЗ №5.** Дослідження практики ЄСПЛ		
8	**Модульний контроль №1**			
ЗМІСТОВНИЙ МОДУЛЬ №2. ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ				
9	**Т №6.** Правове регулювання кібербезпеки в Україні	**Л №6.** Національна система кібербезпеки: засади розбудови.	РН № 3	МК №2
10		**ПЗ №6.** Дослідження законодавства України в сфері кібербезпеки		
11	**Т №7.** Об'єкти та суб'єкти кібербезпеки та їх повноваження в Україні	**Л №7.** Об'єкти та суб'єкти кібербезпеки та їх повноваження в Україні	РН № 3	МК №2
12		**ПЗ №7.** Дослідження комунікаційних систем всіх форм власності; об'єктів критичної інформаційної інфраструктури; комунікаційних системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.		
13	**Т №8.** Департамент кібербезпеки в України, Національний координаційний центр кібербезпеки та Кіберполіція: основні задачі та функції	**Л №8.** Діяльність основних суб'єктів національної системи кібербезпеки	РН № 3	МК №2
14		**ПЗ №8.** Дослідження діяльності структурних підрозділів національної системи кібербезпеки	РН № 3	МК №2
14	**Т №9.** Взаємодія державних органів та приватних компаній у сфері кібербезпеки	**Л №9.** Взаємодія державних органів та приватних компаній у сфері кібербезпеки	РН № 4	МК №2
15		**ПЗ №9.** Дослідження та складання договорів співробітництва та інш. у сфері кібербезпеки	РН № 4	МК №2
15	**Т №10.** Відповідальність за порушення законодавства з кібербезпеки	**Л №10.** Відповідальність за порушення законодавства з кібербезпеки	РН № 4	МК №2
16		**ПЗ №10.** Дослідження та складання процесуальних документів		
16	**Модульний контроль №2**			

6. Самостійна робота здобувача вищої освіти

Важливим елементом опанування змісту дисципліни є самостійна робота здобувачів під керівництвом викладача. Вона передбачає опрацювання навчальної літератури з дисципліни, наукової літератури й аналітичних даних за темою наукових досліджень здобувача, робота з комп'ютером, виконання письмових завдань, опрацювання лекційного матеріалу, підготовка до семінарських і практичних занять, оформлення проведених наукових досліджень у вигляді тез наукових конференцій та наукових статей.

Підготовка до виступів за темами власних досліджень із дотриманням вимог щодо проведення та оформлення результатів наукових досліджень у вигляді тез, наукових статей, препринту.

Політика та контроль

7. Політика навчальної дисципліни

Організація освітнього процесу

Згідно графіку навчального процесу, за розкладом занять, який розміщено на офіційному сайті МНТУ.

Правила відвідування занять

Здобувачі вищої освіти мають відвідувати аудиторні заняття згідно з розкладом, без запізнень. Освітня діяльність та відвідування здобувачами вищої освіти занять регламентується «Правилами внутрішнього розпорядку для студентів МНТУ».

Пропущені заняття відпрацьовуються в часи самостійної підготовки та у встановлені викладачем терміни.

Відвідування лекцій, практичних занять, а також відсутність на них, не оцінюється. Проте, здобувачам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал та демонструються різноманітні методи розв'язування прикладних задач, розвиваються навички та вміння в області забезпечення безпеки інформаційних систем.

Правила поведінки на заняттях

Норми етичної поведінки учасників академічної спільноти визначені у Кодексі академічної етики ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила захисту практичних робіт

Звіти з практичних робіт, оформлені у відповідності до вимог методичних рекомендацій, повинні бути захищені не пізніше наступного практичного заняття. Звіт з останнього практичного заняття повинен бути захищений до дня захисту індивідуального завдання.

Захист звітів з практичних робіт може проводитись: безпосередньо під час поточного практичного заняття, на наступному практичному занятті, у час, що відведений для консультацій.

Процедура оскарження результатів контрольних заходів оцінювання

Після отримання коментарів від викладача з аргументацією щодо оцінки, здобувач вищої освіти має право в індивідуальному порядку задати всі питання, які його/її цікавлять стосовно результатів контрольних заходів оцінювання. Якщо здобувач вищої освіти категорично не погоджуються з оцінкою, він/вона мають також навести аргументи щодо своєї позиції.

Порядок подання апеляційних скарг на результати підсумкового контролю визначено у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Правила призначення заохочувальних та штрафних балів

Заохочувальні бали		**Штрафні бали**	
Критерій	**Бал**	**Критерій**	**Бал**
Участь у міжнародних, всеукраїнських або інших заходах (конкурсах) за тематикою навчальної дисципліни	3 бали	Порушення термінів виконання та захисту звітів з практичних робіт (за кожну роботу)	-2 бали
Опитування на лекційному занятті (опитування на одному занятті)	2 бали	Порушення термінів виконання практичних робіт	-4 бали
Вдосконалення навчально-матеріальної бази кафедри	≤ 5 балів		
Участь у роботі наукового гуртка кафедри за тематикою навчальної дисципліни	5 балів	Злісне невиконання мір техніки безпеки при проведенні навчальних занять (за кожний випадок)	-5 балів

Політика дедлайнів та перескладань

Усі завдання виконуються у зазначені дати та час. Здобувачі несуть відповідальність за управління своїм часом, щоб завдання та проекти могли бути подані до встановленого терміну.

Політика перескладань визначена у Положенні про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у ЗВО «Міжнародний науково-технічний університет імені академіка Юрія Бугая».

Загальна оцінка після перескладання (ліквідації академічної заборгованості) знижується на 10%.

Політика щодо академічної доброчесності

Обов'язкове дотримання академічної доброчесності та недопущення плагіату під час виконання завдань.

Дотримання умов «Положення про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ЗВО «МНТУ» та Кодексу академічної етики.

Списування під час виконання контрольних робіт та модульних тестів заборонені.

Плагіат у творчих роботах та презентаціях – заборонений.

8. Види контролю та рейтингова система оцінювання результатів навчання

Рейтингова система оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до:

– Положення про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у закладі вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»;

– умов і критеріїв, визначених у цьому силабусі.

Система оцінювання та вимоги

Система оцінювання навчальної дисципліни	Оцінювання упродовж кожного змістовного модуля здійснюється за 100 бальною системою (до 40 балів за поточний контроль, до 60 балів за модульний контроль).
Практичні заняття	Максимальна кількість балів за кожне практичне заняття – 5 балів.

	0 балів – не виконання відповідного завдання без поважних причин. 2 бали – виконання відповідних завдань без оформлення звіту. 3 бали - виконання завдання та оформлення звіту з незначною кількістю помилок. 4 бали - виконання завдання, оформлення та захист звіту з кількома негрубими помилками. 5 балів – виконання завдання, оформлення та захист звіту без помилок. При здійсненні оцінювання враховуються наявні штрафні бали для даного заняття.
Умови допуску до підсумкового (модульного) контролю	Виконання всіх практичних завдань за відповідним змістовним модулем. Наявність не менше 20 балів за поточну успішність.

Середньозважений бал за навчальну дисципліну визначається як середній арифметичний бал всіх результатів модульних контролів.

Оцінювання навчальних досягнень здобувачів вищої освіти за всіма видами контролю – здійснюється за національною системою та ECTS.

Шкала оцінювання успішності студентів

СУМА БАЛІВ	ОЦІНКА ECTS	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		екзамен	**залік**
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно	не зараховано
34-0	F	незадовільно	

9. Додаткова інформація з дисципліни (за потреби)

Силабус навчальної дисципліни:
складено доцентом кафедри права, кандидатом юридичних наук
Юлією ДЕРКАЧЕНКО

«Погоджено»
Завідувач кафедри права  Анна НЕЧАЙ