ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
підпис
«31» _____ 2021 р.

СИЛАБУС
Навчальна дисципліна: "Кібернетичне право"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Кравчук Степан Йосипович
Профайл викладач(ів)	http://pravo.khnu.km.ua/profesorsko-vykladatskyj-sklad/
E-mail викладача(ів)	St_kravchuk@ukr.net
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=7306
Навчальний рік, семестр	2021-2022, семестр VI (зимово-весняний)
Розклад	
Консультації	

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	3	6	4	120	51	17	-	34	-	69	-	-	+	-

Анотація дисципліни

Навчальна дисципліна «Кібернетичне право» – складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека», є однією з профілюючих дисциплін. При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, розвитку критичного мислення, модульно-розвивальні.

Пререквізити: громадянське суспільство, економіка та управління.

Кореквізити: управління інформаційною безпекою.

Мета і завдання дисципліни

Мета дисципліни. Надання знань з основ правових явищ, формування комплексного уявлення про основні положення відносин у кібербезпеці; з'ясування засад юридичного забезпечення правової діяльності кібербезпеки.

Предмет дисципліни. Правові відносини в кібербезпеці, найбільш загальні закономірності виникнення, розвитку і функціонування правового регулювання кібербезпеки, а також система правових понять і категорій в сфері інформаційних технологій.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека»:

компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. 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.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

результати навчання:

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки.

РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* знання у практичних ситуаціях, пов'язаних з діяльністю на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки, та при підготовці пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; розуміти предметну область та професію при застосуванні

національних та міжнародних регулюючих актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки; *використовувати* результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; *усвідомлювати* цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні та *реалізовувати* свої права і обов'язки як члена суспільства.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема практ. роботи**	Самостійна роботи		
			Зміст	Год.	Література
1	**Правовий захист інформації** Призначення і структура правового забезпечення захисту інформації. Методи правового захисту інформації. Основні законодавчі акти, правові норми і положення, що регулюють процеси захисту інформації.	-	Опрацювання теоретичного матеріалу лекції №1.	4	[1] с. 8-30 [3] с. 19-38 [4] с. 1-74
2	-	**СЗ №1 Діяльність на основі нормативно-правового забезпечення захисту інформації.** Законодавство України про інформацію. Нормативно-правові акти у сфері захисту інформації. Інформаційна безпека як інтегральна проблема. Концептуальна модель інформаційної безпеки.	Підготовка до СЗ№1.	4	[2] с. 60-71 [6] с. 1-29

3	**Інтелектуальна власність та її захист** Поняття інтелектуальної власності, її види та основні об'єкти освіти. Інтелектуальний продукт, як об'єкт інтелектуальної власності і предмет захисту. Зміст цивільно-правових норм в області захисту інтелектуальної власності. Авторське право. Патентне право. Товарний знак. Договірне право, авторські і ліцензійні договори.	-	Опрацювання теоретичного матеріалу лекції №2.	4	[6] с. 29-37, с. 60-77, с. 80-83
4	-	**СЗ №2 Поняття права інтелектуальної власності.** Загальна характеристика авторського права та суміжні права. Засоби індивідуалізації власників інформаційних активів, як об’єкту права інтелектуальної власності.	Підготовка до семінарського заняття №2.	4	[2] с. 60-71 [6] с. 37-60 [7] с. 22-35
5	**Види інформації за порядком доступу** Види інформації. Правовий режим та порядок доступу до інформації. Публічна інформація. Інформація з обмеженим доступом.	-	Опрацювання теоретичного матеріалу лекції №3.	4	[6] с. 77-90

6	-	**СЗ №3 Законодавче регулювання доступу до різних видів інформації.** Суб'єкти відносин у сфері доступу до публічної інформації та інформації з обмеженим доступом. Реалізація права на доступ до публічної інформації, інформаційний запит. Правові особливості доступу до інформації з обмеженим доступом.	Підготовка до СЗ №3.	4	[1] с. 105-118 [6] с. 90-107
7	**Інститути державної, банківської, комерційної та інших видів таємниць** Правові основи захисту державної, комерційної, службової, професійної та особистої таємниці, персональних даних. Організаційно-правові методи охорони державної таємниці, захисту комерційної, службової, професійної та особистої таємниці, персональних даних.	-	Опрацювання теоретичного матеріалу лекції №4.	4	[8] с. 1-26

8	-	**СЗ №4 Правові заходи, щодо охорони державної, банківської та комерційної таємниці.** Державні органи в сфері захисту державної таємниці. Режимно-секретні органи, їх правовий статус та завдання. Співвідношення банківської та комерційної таємниць. Підготовка пропозицій до нормативних актів щодо забезпечення державної, банківської та комерційної таємниці.	Підготовка до СЗ №4.	4	[5] с. 1-23 [7] с. 10-17
9	**Кримінальна, цивільно-правова, адміністративна і дисциплінарна відповідальність за розголошення інформації, що захищається** Види і умови застосування правових норм кримінальної, цивільно-правової, адміністративної та дисциплінарної відповідальності за розголошення інформації, що захищається і невиконання правил її захисту. Правові проблеми, пов'язані із захистом прав власників власності на інформацію та розпорядженням інформацією.	-	Опрацювання теоретичного матеріалу лекції №5.	4	[9] с. 1-45

10	-	**СЗ №5 Відповідальність за розголошення інформації, що захищається.** Відповідальність за порушення законодавства про охорону державної таємниці. Відповідальність за порушення законодавства про захист банківської та комерційної таємниць. Відповідальність за порушення законодавства про захист персональних даних. **Тестування**	Підготовка до СЗ №5. Підготовка до тестування	4	[1] с. 119-127 [10] с. 7-33 [11] с. 21-31
11	**Правове регулювання взаємовідносин адміністрації і персоналу в області захисту інформації** Правове регулювання взаємовідносин адміністрації і персоналу в області захисту інформації: основні поняття, нормативно-правові акти і положення.	-	Опрацювання теоретичного матеріалу лекції №6.	4	[2] с. 74-92 [15] с. 24-38
12	-	**СЗ №6 Правове регулювання взаємовідносин адміністрації і персоналу в області захисту інформації.** Правові основи роботи з персоналом. Підготовка пропозицій до нормативних актів щодо підбору персоналу для роботи з таємною інформацією.	Підготовка до СЗ №6.	4	[2] с. 114-123 [11] с. 31-36, с. 42-48 [12] с. 55-95

13	**Правова діяльність підрозділів захисту інформації** Правові основи діяльності підрозділів захисту інформації. Роль права в регулюванні комплексу відносин в сфері захисту інформації.	-	Опрацювання теоретичного матеріалу лекції №7.	4	[13] с. 47-60 [14] с. 52-122
14	-	**СЗ №7 Діяльність підрозділів захисту інформації.** Основні функції даних підрозділів. Підготовка пропозицій до нормативних актів щодо діяльності підрозділів захисту інформації на підприємстві.	Підготовка до СЗ №7.	4	[13] с. 47-60 [14] с. 74-122
15	**Досудове розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки/ кібербезпеки** Інциденти інформаційної безпеки та кібербезпеки: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози. Особливості кримінального та інших видів проваджень. Захист та охорона таємниці досудового розслідування.	-	Опрацювання теоретичного матеріалу лекції №8.	4	[2] с. 124-163

16	-	**СЗ№8 Розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки/ кібербезпеки.** Правовий інститут досудового розслідування. Процесуальні та матеріальні норми права. Межі застосування досудового розслідування. Фіксування розслідування технічними засобами, збір доказів. Недосконаліть законодавства щодо досудового розслідування, пропозиції щодо його покращення. **Контрольна робота**	Підготовка до СЗ №8. Підготовка до контрольної роботи	6	[12] с. 8-55 [15] с. 38-56, с. 85-92
17	**Міжнародний досвід в сфері захисту інформації та в боротьбі з комп'ютерною злочинністю** Комп'ютерна злочинність та її характерні риси. Види комп'ютерних злочинів. Загальна характеристика комп'ютерних злочинців. Міжнародний досвід боротьби з загрозами інформаційної та кібербезпеки і протидії комп'ютерній злочинності.	-	Опрацювання теоретичного матеріалу лекції №9.	4	[15] с. 11-31, с. 87-164

*** лекції проводяться по 2 години раз на два тижні;**
**** семінари проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, семінарські заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати контрольні точки. Пропущене з поважної причини практичне заняття студент повинен відпрацювати у встановлений викладачем термін.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

Опис самостійного завдання (реферату)

Важливим принципом самостійної роботи є індивідуальна робота кожного студента. Її призначенням є: поглиблення теоретичних знань, отриманих на лекціях; заохочення студентів до аналізу нормативно-правових джерел, активної творчої роботи із опрацюванням рекомендованої літератури; забезпечення майбутніх фахівців усіх напрямів підготовки знаннями основних правових положень, що стосуються їх професійної діяльності; формування у студентів вміння орієнтуватися в нормативних джерелах; вироблення у майбутніх спеціалістів практичних навичок реалізації норм чинного законодавства.

Індивідуальна робота передбачає підготовку реферату з обраної студентом тематики а також підготовку до семінарсько-практичних занять протягом семестру.

Виконання індивідуального завдання включає в себе п’ять основних етапів:

1) вибір теми дослідження;
2) підбір матеріалів;
3) опрацювання літератури;
4) написання тексту;
5) оформлення роботи.

Індивідуальна робота є складовою вивчення змісту навчальної дисципліни та будується на рівнях творчого пошуку та критичного мислення. Вона сприяє розвитку творчої активності студентів, прищеплює навички, необхідні для самоосвіти, пошуку шляхів вдосконалення професійної діяльності після закінчення навчання.

Теми індивідуальної роботи мають науково-дослідний характер, підвищену складність, виступають певним тематичним доповненням семінарського заняття, методом поглибленої підготовки до нього і можуть готуватись у вигляді реферативних повідомлень.

Реферат готується у письмовому викладі, має науковий характер і здійснюється шляхом аналізу різних інформаційних джерел. Теми рефератів наведені у планах семінарських занять. Він повинен мати чітку логічну побудову і повинен містити наступні елементи:

1. Титульний аркуш.
2. План роботи із зазначенням сторінок початку кожного з розділів.
3. Вступ на 1–2 сторінки (аналізується проблема та стан її дослідження науковцями).
4. Основна частина обсягом 8–10 сторінок (викладається основний матеріал).
5. Висновки на 1–2 сторінки.
6. Перелік використаних джерел.
7. Реферат може містити додатки, переліки умовних скорочень тощо.

У вступі обґрунтовується актуальність обраної теми, дається коротка характеристика сучасного стану і наукової розробки проблеми (питання), що розглядатиметься в рефераті, формулюється мета роботи, а також здійснюється короткий огляд джерел, використаних студентом.

Основна частина передбачає розкриття змісту обраної теми, її основних питань і проблем. Головною вимогою є аналіз проблем, відображених у літературі, висвітлення різних позицій науковців та їх критичний аналіз. При підготовці студенту студент повинен продемонструвати уміння самостійно робити висновки на основі вивчених нормативно-правових актів та літератури й узагальнювати матеріал. Основна частина може складатися з двох–трьох розділів.

У заключній частині у стислому вигляді подаються висновки, які містять короткий підсумок проведеного дослідження, тобто є коротким резюме реферату, а також підтверджується вирішення поставлених завдань і досягнення мети. Тут повинні надаватись рекомендації і пропозиції щодо практичного розв’язання розглянутих проблем. Наприкінці реферату вміщують список використаних джерел, додатки (за необхідності). Складові частини роботи мають логічно поєднуватися і відповідати одна одній.

Література з теми реферату повинна мати пізнавальне значення у контексті вивчення та осмислення дисципліни, тому до списку варто включати монографії, статті з наукових журналів, навчальні посібники, що рекомендовані навчальною та робочою програмами або знайдені автором роботи, документальні та інформаційні джерела тощо. Матеріали у списку слід оформляти згідно з державними стандартами України.

Робота виконується на стандартних аркушах ф. А4 грамотно, без помарок і виправлень. Скорочення слів, окрім узвичаєних абревіатур, не допускається. Текст розміщують на одній стороні аркуша, залишаючи поля з усіх боків по 2 см.

Першою сторінкою реферату є титульний аркуш, де вказується тема, прізвище, ім'я та по-батькові автора, спеціальність, курс, група. На другій сторінці повинен бути наведений план реферату із зазначенням сторінок, де починаються відповідні розділи. Кожний розділ починається з нової сторінки. Сторінки нумеруються, починаючи з титульного аркуша, однак номери проставляються тільки з другої сторінки (таким чином, вступ зазвичай починається на 3-й сторінці). Розділи основної частини нумеруються арабськими цифрами, параграфи – цифрою розділу і параграфа через крапку (1.2, 2.2 і т.п.). Вступ і висновки не нумеруються.

Назву таблиць вказують зверху над таблицею, а назву малюнків розміщують під малюнком. Нумерація таблиць і малюнків може бути наскрізною по всій роботі.

При підготовці реферату ставиться наступна мета:

– систематизація, закріплення та розширення отриманих теоретичних знань за фахом і їхнім застосуванням для постановки і рішення конкретних наукових і прикладних (практичних) завдань;

– поглиблення навичок ведення самостійної роботи, оволодіння сучасними методами постановки і аналізу проблем;

– уміння критично аналізувати літературу, творчо обговорювати результати роботи, вести наукову полеміку.

Реферативна робота повинна:

– мати творчий характер з використанням актуальних статистичних даних і діючих нормативних правових актів;

– відповідати вимогам логічного і чіткого викладу матеріалу, доказовості і вірогідності фактів;

– відображати вміння студента користуватися раціональними прийомами пошуку, відбору, обробки та систематизації інформації, здатності працювати з нормативно-правовими актами.

Індивідуальне завдання студенти виконують під керівництвом викладача в позаурочний час. Якість виконання враховується при виставленні підсумкової семестрової оцінки.

Тематика рефератів для самостійної роботи студентів

1.Закономірності та засади формування кіберправа;
2. Забезпечення прав і свобод людини і громадянина, законних інтересів суспільства і держави у сфері кіберправа;
3. Кіберзаконодавство, проблеми, пріоритети, напрями розвитку;
4. Рулювання охорони і захисту персональних даних у кіберсфері;
5. Запобігання, виявлення і припинення правопорушень (злочинів) в кіберсфері;
6. Відповідальність за вчинення правопорушень (злочинів) в кіберсфері
7. Кіберзлочини та кіберзагрози;
8. Обшуки, перевірки, тимчасовий доступ під час розслідування кібезлочинів;
9. Кримінально-процесуальні аспект розслідування кібезлочинів;
12. Персональні дані, як складова права на приватність;
13. Відповідальність за порушення законовства про персональні дані;
14. Захист персональних даних в соціальних мережах;
15. Конфіденційність інформації у мережі Інтернет;
16. Правові проблеми віртуального середовища;
17. Юридичні аспекти захисту авторських прав у мережі Інтернет та відповідальність за порушення умов використання контенту;

18. Концептуальна модель захисту таємниці досудового розслідування;
19. Комп'ютерна злочинність, як комплексна загроза інформації;
20. Промислове шпигунство, як загроза комерційній таємниці.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ У СЕМЕСТРІ

Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**		**Самостійна робота**	**Підсумковий контрольний захід**
Вид заняття	Семінарські заняття (мінімальна кількість оцінок - 6)	Тестування	Контрольна робота	Реферат	Залік за рейтингом
Тема	1-9	1-5	6-9	-	
Ваговий коефіцієнт	0,2	0,2	0,4	0,2	

Оцінювання семінарських занять (усне опитування, практична перевірка). Оцінка, яка виставляється за семінарське заняття, складається з таких елементів: знання теоретичного матеріалу з теми; вільне володіння студентом спеціальною термінологією і уміння застосовувати знання на практиці; активність під час обговорення теми.

Оцінку за практичне заняття викладач оголошує в кінці заняття та проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тестове завдання для кожного студента складається з десяти тестів, кожен з яких оцінюється чотирма балами. Максимальна сума балів, яку може набрати студент, складає 40.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту, представлена у нижченаведеній таблиці.

Сума балів за тестове завдання	1 – 10	11-20	21-30	31-40
Оцінка	2	3	4	5

Якщо відповідь на тестове завдання має 2-3 правильних значення, а студент зумів вказати частину з них, то сума балів у цьому випадку буде пропорціональна кількості правильних відповідей. Наприклад, у тесті є три правильних відповіді, а студент вказав лише дві з них, тоді він отримує за тестове завдання два бали з трьох.

На тестування відводиться 15 хвилин. Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей повинні бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей. Викладач на наступному занятті оголошує результати тестування.

Оцінювання контрольних робіт з дисципліни. Контрольна робота складається з 3 питань, кожен з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, становить 3.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за контрольну роботу оцінці, що виставляється студенту, представлена у наведеній таблиці.

Сума балів за контрольну роботу	0,50-1,00	1,50-2,00	2,15-2,50	3
Оцінка	2	3	4	5

Якщо студент зумів дати відповідь на частину з них, то сума балів у цьому випадку буде пропорціональна кількості правильних відповідей. Наприклад, у варіанті є три питання, а студент вказав лише правильну вичерпну відповідь на одне з них, тоді він отримує за завдання 1 бал, має незначні неточності – 0,75 , неповна – 0,5, поверхнева – 0,25.

На контрольну роботу відводиться 20 хвилин. Результати оголошуються на наступному занятті.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх

	зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Студент, який не набрав позитивний середньозважений бал за поточну роботу або не виконав індивідуальний план з дисципліни повністю, вважається невстигаючим.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незарахо-вано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ ЗНАНЬ

1. Визначення «кібернетичне (інформаційне) право»
2. Принципи кібернетичного (інформаційного) права
3. Базовий принцип інформаційного права
4. Об’єкт інформаційного права
5. Предмет інформаційного права
6. Визначення (поняття) «метод інформаційного права»
7. Складові методу інформаційного права
8. Методи інформаційного права як науки
9. Методи інформаційного права як галузі права
10. Методи інформаційного права як навчальної дисципліни
11. Визначення «імперативного методу правового регулювання інформаційних відносин»
12. Визначення «диспозитивного методу правового регулювання інформаційних відносин»
13. Складові імперативного методу правового регулювання інформаційних відносин
14. Складові диспозитивного методу правового регулювання інформаційних відносин
15. Практичне значення застосування імперативного та диспозитивного методів
16. Класифікація відносин в інформаційній сфері та їх склад
17. Визначення «інститут інформаційного права»
18. Склад основних інститутів інформаційного права відповідно до процесу створення інформації
19. Склад основних інститутів інформаційного права відповідно до процесу поширення інформації
20. Склад основних інститутів інформаційного право відповідно до процесу забезпечення мінімізації збитку від несанкціонованого поширення, використання і знищення інформації
21. Склад інституту захисту інформації
22. Основні принципи інформаційних відносин
23. Основні напрями державної інформаційної політики
24. Основні види інформаційної діяльності
25. Види інформації за змістом
26. Види інформації за порядком доступу
27. Види інформації з обмеженим доступом
28. Суб’єкти відносин, пов’язаних із захистом інформації в інформаційно-телекомунікаційних системах
29. Суб’єкти інформаційних відносин
30. Правовий режим інформаційних ресурсів
31. Мета організаційно-правового забезпечення захисту інформації
32. Зміст організаційно-правового забезпечення захисту інформації
33. Система документів організаційно-правового забезпечення захисту інформації
34. Джерела кібернетичних загроз
35. Різновиди кіберзлочинів
36. Зміст Конвенції Ради Європи про кіберзлочинність
37. Мета Конвенції Ради Європи про кіберзлочинність
38. Класифікація кіберзлочинів відповідно до Конвенції Ради Європи про кіберзлочинність.
39. Зміст злочинів проти конфіденційності, цілісності і доступності комп’ютерних даних та систем відповідно до Конвенції Ради Європи про кіберзлочинність
40. Зміст злочинів, пов’язаних з використанням комп’ютерів, відповідно до Конвенції Ради Європи про кіберзлочинність
41. Визначення «злочину» відповідно до Кримінального кодексу України
42. Кримінальна відповідальність за скоєння кіберзлочинів
43. Адміністративна відповідальність за скоєння правопорушень

44. Визначення «адміністративного правопорушення» відповідно до Кодексу України про адміністративні правопорушення
45. Інциденти інформаційної безпеки та кібербезпеки: характерні ознаки та проблемні аспекти
46. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози
47. Особливості кримінального та інших видів проваджень
48. Захист та охорона таємниці досудового розслідування.
49. Правове регулювання взаємовідносин адміністрації і персоналу в області захисту інформації: основні поняття, нормативно-правові акти і положення.
50. Правові основи діяльності підрозділів захисту інформації.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Кібернетичне право» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Герц А.А., Кравчук С.Й. Правознавство: навч. посібник. Київ: Кондор, 2018. 288 с.	Кафедра права
2.	Кравчук С.Й. Господарське право України: навч. посібник. Київ : Кондор. 2009. 228 с.	https://www.twirpx.com/file/158533/
3.	Мазур О.С. М Цивільне право України: Навч. Пос. / О.С. Мазур. — К.: Центр навчальної літератури, 2006. — 384 с.	http://library.nlu.edu.ua/POLNTEXT/CUL/46-Civilne_pravo_Mazur.pdf
4.	Т. В. Бачинський, Р. І. Радейко О. І., Харитонова О.І. Основи ІТ права / Т.В. Бачинський, О.І. Радейко,О.І. Харитонова – К: Юрінком Інтер. 2019. -224 с.	Кафедра права
5.	ІТ право / Яворська Л.С., Тарасенко Л.Л., Мартин В.М., Самагальська Ю.Я. та ін. / За заг. ред. Яворської О.С. – Львів: Видавництво «Левада», 2017. – 470 с.	http://tspartners.lviv.ua/userfiles/IT%20ПРАВО%20ПІДРУЧНИК%202017(1).pdf
6.	Право інтелектуальної власності: Академічний курс / За ред. О.А. Підопригори, О. Д. Святоцького. — Вид. друге, перероб. та доповн. — К.: Видавничий Дім «Ін Юре», 2004.- 341 с.	Кафедра права
7.	Право інтелектуальної власності в Інтернеті : [наук.-практ. посібник] / С.А. Петренко, В.М. Троцька. – К.: НДІ інтелектуальної власності НАПрНУ, «НВП «Інтерсервіс», 2013. – 288 с.	Кафедра права
8.	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.	http://www.dut.edu.ua/uploads/p_303_79299367.pdf
9.	Селезньова О.М. Теоретико-методологічні основи інформаційного права України : [монографія] / О. М. Селезньова. - Чернівці: Місто, 2014. - 408 с.	http://aphd.ua/publication-164/
10.	Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 [Електронний ресурс].	http://zakon5.rada.gov.ua/laws/show/994_5 75
11.	Кримінальний кодекс України. Верховна Рада України; Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III [Електронний ресурс].	https://zakon.rada.gov.ua/laws/show/994_575#Text
12.	Закон України «Про Національну програму інформатизації» [Електронний ресурс].	http://zakon3.rada.gov.ua/laws/show/74/98-ep
13.	Закон України «Про інформацію», Верховна Рада України; Закон від 02.10.1992 №2657-XII [Електронний ресурс].	http://zakon3.rada.gov.ua/laws/show/2657-12
14.	Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. - Київ: ДСТСЗІСБ України, 1999. - 26 с.	https://tzi.com.ua/nd-tz-1.1-003-99.html
15.	Правовий захист інформації: Навчальний посібник / Н.І. Логінова, Р.Р. Дробожур. - Одеса: Фенікс, 2015. - 264 с.	http://dspace.onua.edu.ua/bitstream/handle/11300/1824/Правовий%20захист%20інформації.%20Логінова%2C%20Дробожур.pdf?sequence=1&isAllowed=y

Додаткова

16.	Атаманова Ю.Є. Захист прав інтелектуальної власності у мережі Інтернет: світовий досвід та вітчизняні перспективи. //Атаманова Ю.Є. Право та інновації. 2014. № 3.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=apir_2014_3_3

17.	Аврамова О.Є., Разіна О.І. Проблеми захисту авторських прав в інтернеті // Вісник НТУ «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства. – Харків: НТУ «ХПІ», 2013. – № 6(980). – С. 26-29.	http://repository.kpi.kharkov.ua/handle/KhPI-Press/2764
18.	Горкуша М. Захист авторських та суміжних прав, порушених в мережі Інтернет // Інтелектуальна власність. – 2014. – № 6.	https://www.academia.edu/32942280/Горкуша_М_Ю_Захист_авторських_та_суміжних_прав_порушених_в_мережі_Інтернет_М_Ю_Горкуша_Інтелектуальна_власність_в_Україні_2014_6_c_36_46
19.	Грігор'янц Г. І. Захист авторських і суміжних прав від піратства в мережі інтернет за законодавством України та Російської Федерації // Актуальні проблеми держави і права. – Одеса. – 2014. – № 72. – С.236-242.	http://dspace.onua.edu.ua/handle/11300/4519
20.	Дмитришин В.С. Набуття та передання прав на комп'ютерні програми: автореф. дис… канд. юрид. наук: 12.00.03 / Дмитришин В. – Інститут держави і права ім. В.М.Корецького Національної академії наук України. – Київ, 2008.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=ARD&P21DBN=ARD&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A=&S21COLORTERMS=1&S21STR=Дмитришин%20В.С.$
21.	Катеринчук К. Порушення авторського права: як відрізнити некоректне та неправомірне цитування від плагіату? // Юридичний журнал. – 2013. – № 2.	http://www.justinian.com.ua/article.php?id=3822
22.	Рудник Т.В. Відповідальність за порушення авторського права // Часопис Київського університету права. – Київ. – 2012. – № 2. – С.248-251.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Chkup_2012_2_61
23.	Тарасенко Л.Л. Захист авторських прав: процесуальні аспекти /Л.Л.Тарасенко // Часопис Київського університету права: Український науково-теоретичний часопис. – К.: Київ. Ун-т права НАН України, Ін-т держ. і права ім. В.М.Корецького НАН України. – 2015. – № 2. – С.246-250	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Chkup_2015_2_60
24.	Тарасенко Л.Л. Суб'єктний склад розгляду справ щодо захисту авторських прав /Л.Л.Тарасенко // Науковий вісник Ужгородського національного університету. Серія «Право». – Ужгород: Ужгородський нац. ун-т, 2015. – Вип. 34. – Т. 1.– С.105-109.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=nvuzhpr_2015_34(1)__28
25.	Штефан О. Позов у справах, що виникають з авторських правовідносин // Журнал "Теорія і практика інтелектуальної власності" . – 2014. – № 3. – С.12-25.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Tpiv_2014_3_3

Інформаційні ресурси:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ (Підпис) к.ю.н., доцент (Вчений ступінь, звання) С.Й. Кравчук (Ініціали, прізвище викладача(ів))

Погоджено
Гарант освітньої програми _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) В.М. Чешун (Ініціали, прізвище)

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Ю.П. Кльоц (Ініціали, прізвище)