Національний юридичний університет імені Ярослава Мудрого

Кафедра кримінології та кримінально-виконавчого права

С И Л А Б У С

навчальної дисципліни

«Запобігання кіберзлочинам»

Рівень вищої освіти – перший (бакалаврський) рівень

Ступінь вищої освіти – бакалавр

Галузь знань – 08 «Право»

Спеціальність – 081 «Право»

Статус навчальної дисципліни – за вибором студента

Рік набору - 2020

Харків – 2020

Силабус навчальної дисципліни «Запобігання кіберзлочинам» для здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2020. 17 с.

Розробник:

Таволжанський Олексій Володимирович

доцент, кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права

Затверджено на засіданні кафедри

кримінології та кримінально-виконавчого права,

(протокол № 1 від 03 вересня 2020 р.)

Завідувач кафедри -Головкін Богдан Миколайович, доктор юридичних наук, професор

Дані про викладача

Назва навчальної дисципліни	Запобігання кіберзлочинам
Статус навчальної дисципліни	За вибором студента
Викладач	**Таволжанський Олексій Володимирович,** доцент, кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права
Контактний телефон	0577049262
E-mail	criminology@nlu.edu.ua
Консультації	відповідно до графіку індивідуальних консультацій
Онлайн консультації	Zoom-ідентифікатор 338 563 0000, код доступу 111471

Анотація навчальної дисципліни

Розкривається закономірності виникнення, поширення та відтворення кіберзлочинності у суспільстві, організаційно-правовий механізм запобігання кіберзлочинам, розуміння основних категорій і понять національної система кібербезпеки. Аналізується зміст і значення принципів забезпечення кібербезпеки. Окреслюється коло суб'єктів які займаються запобіганням кіберзлочинів, встановлюються їх права й обов'язки. Послідовно розглядається, а також аналізуються особливості запобігання окремих видів кіберзлочинів.

Мета та завдання навчальної дисципліни

Мета навчальної дисципліни – формування системи наукових знань про правове регулювання запобігання кіберзлочинів, вивчення вітчизняних та зарубіжних підходів до розуміння змісту заходів забезпечення кібербезпеки, вироблення основних умінь і навичок застосування національного законодавства, активізація аналітичної діяльності студентів, проведення науково-дослідницької роботи, а також практичних навичок діяльності правника.

Завдання:

– формування знань про кіберзлочинність, системи теоретичних знань про інститут кібербезпеки, його змістовне наповнення;

- опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки;

- визначення стану кіберзлочинності: рівня, структури, динаміки та інших показників;

– осмислення змісту актуальних проблем дослідження особи кіберзлочинця, формування криміногенної спрямованості особистості та мотивації кримінальної поведінки, типології і класифікації злочинців у віртуальній сфері;

- аналіз і дослідження прикладних проблем порядку формування та реалізації державної політики в сфері забезпечення кібербезпеки, спрямованих на набуття (підтвердження) суб'єктивних прав та покладення на приватних осіб передбачених законом обов'язків;

- наведення характеристики класифікацій та видів кіберзлочинів, аналіз їх структури, визначення стадій та етапів, окреслення повноважень суб'єктів запобігання кіберзлочинам;

- розвиток навичок і умінь запровадження та застосування заходів запобігання кіберзлочинам.

Навчальна дисципліна у структурі освітньо-професійної програми. Міждисциплінарні зв'язки

Пререквізити: «Теорія права», «Логіка», «Історія держави і права України».

Кореквізити: «Адміністративне право», «Кримінальне право (Загальна частина)», «Кримінальне право (Особлива частина)», «Кримінальний процес».

Постреквізити: ----

Очікувані результати навчання здобувача вищої освіти

РН НД 1. Пояснювати соціально-правову природу кіберзлочинності.

РН НД 2. Демонструвати вміння аналізувати рівень, структуру і динаміку кіберзлочинності

РН НД 3. Визначати й аналізувати причини та умови вчинення кіберзлочинів.

РН НД 4. Демонструвати вміння здійснювати типологію і класифікацію кіебрзлочинців.

РН НД 5. Демонструвати знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю.

РН НД 6. Демонструвати комплексні знання основ забезпечення національної безпеки України та кібербезпеки, структури, завдань та повноважень суб'єктів сектору безпеки та оборони України, організаційних засад їх діяльності.

РН НД 7. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти основ національної безпеки України.

РН НД 8. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинності.

РН НД 9. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання терористичній кіберзлочинній діяльності.

РН НД 10. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку.

РН НД 11. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем,

такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

РН НД 12. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів пов’язаних з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо).

Види навчальних занять та самостійна робота
для здобувачів вищої освіти денної форми навчання

№ п/п	Аудиторні заняття (контактні)		Самостійна робота (в годинах)
	Теми лекцій	**Теми практичних занять**	
1.	Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	4
2.	Стан забезпечення кібербезпеки на сучасному етапі.	Стан забезпечення кібербезпеки на сучасному етапі.	10
3.	Поняття і визначення кіберзлочину.	Поняття і визначення кіберзлочину.	12
4.	Кіберзлочинність та її вимірювання.	Кіберзлочинність та її вимірювання.	12
5.	Особа кіберзлочинця.	Особа кіберзлочинця.	12
6.	Запобігання кіберзлочинності: поняття, зміст, значення.	Запобігання кіберзлочинності: поняття, зміст, значення.	12
7.	Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	14
8.	Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)	Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)	12
9.	Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів	Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів	12
10.	Гібридна війна.	Гібридна війна.	14

Види навчальних занять і самостійна робота для здобувачів вищої освіти заочної форми навчання

№ п/п	Теми лекцій	Теми практичних занять	Самостійна робота (в годинах)
1.	Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	156
2.	Стан забезпечення кібербезпеки на сучасному етапі.	Стан забезпечення кібербезпеки на сучасному етапі.	
3.	Поняття і визначення кіберзлочину.	Поняття і визначення кіберзлочину.	
4.	Кіберзлочинність та її вимірювання.	Кіберзлочинність та її вимірювання.	
5.	Особа кіберзлочинця.	Особа кіберзлочинця.	
6.	Запобігання кіберзлочинності: поняття, зміст, значення.	Запобігання кіберзлочинності: поняття, зміст, значення.	
7.	Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	
8.	Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)	Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)	
	Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів	Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів	
	Гібридна війна.	Гібридна війна.	

1 Самостійна робота студентів

Самостійна робота студентів здійснюється у таких формах:

– опрацювання нової наукової та навчальної літератури, статистичних даних і звітів компетентних державних органів;

– самостійне вивчення додаткової літератури та додаткових питань;

– робота над кейсами з питань запобігання кіберзлочинам;

– виконання практичних завдань, самотестування;

– доопрацювання матеріалів лекцій;

– написання есе та рефератів;

– підготовка дослідження з вузькоспеціальної проблематики із подальшою його презентацією перед аудиторією;

– розробка схем, таблиць за темами навчальної дисципліни;

– підготовка та публікація наукових статей, тез наукових доповідей, участь у науково-практичних конференціях тощо;

– тематичне узагальнення правозастосовної практики;

– анотування правових позицій Європейського суду з прав людини;

– участь у конкурсах студентських наукових праць, олімпіадах, турнірах, наукових гуртках;

– підготовка до практичних занять, колоквіумів та тестування.

Завдання та методичні рекомендації до самостійної роботи наведено у Навчально-методичному посібнику для самостійної роботи та практичних занять з навчальної дисципліни «Запобігання кіберзлочинам» для студентів першого (бакалаврського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право.

Навчально-методичне та інформаційне забезпечення навчальної дисципліни

Нормативно-правові акти

Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. URL : https://zakon.rada.gov.ua/laws/show/2341-14/ed20200813#Text .

Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19/ed20200703#Text_

Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20/ed20200816#Text

Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. URL : https://zakon.rada.gov.ua/laws/show/2135-12/ed20200703#Text_

Про організаційно-правові основи боротьби з організованою злочинністю: закон України від 30 червня 1993 року № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12/ed20200703#Text_ .

Про інформацію : Закон України від від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text_.

Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI URL : // https://zakon.rada.gov.ua/laws/show/2297-17/ed20200320#Text

Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text_

Про основні засади забезпечення кібербезпеки України : Закону України від 05.10.2017 р. № 2163-VIII URL : https://zakon.rada.gov.ua/laws/show/2163-19/ed20200703#Text

Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII URL : https://zakon.rada.gov.ua/laws/show/2469-19/ed20200815#Text

Про кіберзлочинність : Конвенція ратифіковано із застереженнями і заявами Законом N 2824-IV ( ) від 07.09.2005, URL : https://zakon.rada.gov.ua/laws/show/994_575#Text_

Література

Бідняк Г.С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.

Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

Карчевський М.В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Науково-теоретичний журнал. 2017. С. 99-08.

Світличний О. П. Право інтелектуальної власності: Підручник. Вид. 2, змін. і доп. К.: Н УБіП України, 2017. 355 с.

Таволжанський О.В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів. Журнал східноєвропейського права. – 2018. - № 56. – С. 90-105.

Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2017. - № 4. - С. 158-164.

Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді). Asia life science, Supplement 21(2), December 2019. Iss. 2. P. 863-879. Філіпини. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85077221643&origin=resultslist

V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, *O. V. Tavolzhanskyi*, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction. Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist

O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi Robotization of manufacturing process: economic and social problems and legal ways of their solution (Роботизація виробничого процесу: економічні і соціальні проблеми та правові шляхи їх вирішення). Financial and credit activity:problems of theory and practice (Фінансово-кредитна діяльність: проблеми теорії та практики). - Харків, 2019. - Том 3, № 30. - С. 454-462. (Web of Science Core Collection)

Ovcharenko, Mykola O., *Tavolzhanskyi, Oleksii V.,* Radchenko, Tetiana M., *Kulyk, Kateryna D., Smetanina, Nataliia V.* Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method (Противодействие незаконному обороту наркотиков через Интернет с помощью метода

профилирования). Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). Румыния. Vol. 11, n. 4 (2020), p. 1296-1304.

Інтернет-ресурси

Офіційний веб-портал Верховної Ради України. URL: http://rada.gov.ua/

Офіційний веб-портал Президента України. URL: http://www.president.gov.ua_

Офіційний веб-портал Кабінету Міністрів України (єдиний веб-портал органів виконавчої влади України). URL: http://www.kmu.gov.ua

Офіційний веб-портал судової влади України. URL: https://court.gov.ua/

Офіційний веб-портал Верховного Суду. URL: https://supreme.court.gov.ua/supreme/gromadyanam/perelik_sprav/

Офіційний веб-портал Конституційного Суду України. URL: https://ccu.gov.ua_

Офіційний веб-портал Міністерства юстиції України. URL: https://minjust.gov.ua_

Офіційний веб-портал Офісу Генерального прокурора. URL: www.gp.gov.ua/

Офіційний веб-портал Національного антикорупційного бюро України. URL: https://nabu.gov.ua/

Офіційний веб-портал Державного бюро розслідувань. URL: https://dbr.gov.ua/

Офіційний веб-портал Міністерства внутрішніх справ України. URL: https://mvs.gov.ua/uk

Офіційний веб-портал Інтерполу. URL: https://www.interpol.int/

Офіційний веб-портал Євроюсту. URL: https://www.eurojust.europa.eu/

Офіційний веб-портал Європейського суду з прав людини. URL: https://www.echr.coe.int/Pages/home.aspx?p=applicants/ukr&c

Офіційний веб-портал Єдиного державного реєстру судових рішень. URL: http://www.reyestr.court.gov.ua/

СЕНМК

Стандартизований електронний навчально-методичний комплекс кафедри кримінології та кримінально-виконавчого права. URL: https://library.nlu.edu.ua/senmk/itemlist/category/199-kafedra-kriminologii-ta-kriminalno-vikonavchogo-prava.html

Вимоги викладача

Здобувачі вищої освіти *повинні*: регулярно відвідувати лекції та практичні заняття; систематично й активно працювати на них; переконливо наводити аргументацію при вирішенні завдань; якісно виконувати письмові завдання, контрольні та самостійні роботи тощо. Практичні заняття, пропущені з поважних причин, можуть бути відпрацьовані за попереднім узгодженням із викладачем.

Здобувачам вищої освіти *рекомендується*: брати участь у науково-практичних конференціях, конкурсах студентських наукових праць, роботі наукового гуртка кафедри, готувати тези наукових доповідей тощо.

Обов'язкова вимога – дотримання здобувачами вищої освіти норм «Кодексу академічної етики Національного юридичного університету імені Ярослава Мудрого» (http://nauka.nlu.edu.ua/wp-content/uploads/2020/08/kodeks_academichnoyi_etyky.pdf).

Під час аудиторних занять дозволяється використовувати ґаджети тільки в навчальних цілях (приміром, для перегляду презентацій лекції), а ноутбуки і планшети – для ведення конспектів лекцій і відстеження потрібної інформації.

Контрольні заходи

Оцінювання результатів засвоєння навчальної дисципліни «Запобігання кіберзлочинам» передбачає проведення поточного та підсумкового контролю і здійснюється на основі накопичувальної бально-рейтингової системи.

Поточний контроль знань включає:

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни на практичних заняттях із застосуванням таких засобів: усне, письмове або експрес-опитування, вирішення практичних завдань або задач, участь у розробці кейсів, захист есе або реферату за ініціативи студента. Поточний контроль має на меті перевірку рівня підготовки студента до вивчення поточного матеріалу. У ході практичного заняття студент може отримати оцінку за чотирибальною шкалою (0, 3, 4, 5);

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни, що проводиться наприкінці модулів у формі колоквіумів або тестових завдань.

Впродовж семестру студенти виконують завдання для самостійної роботи (підготовка презентації, есе, реферату тощо). Максимальна кількість балів за самостійну роботу – 20 балів.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни є залік. Мінімальна кількість балів для отримання заліку – 60 балів (за результатами проведення поточного контролю та оцінювання самостійної роботи студента).

Шкала підсумкового педагогічного контролю

Оцінка за шкалою ECTS	Визначення	Оцінка за національною шкалою	Оцінка за 100-бальною шкалою, що використовується в НЮУ

A	**Відмінно** – відмінне виконання, лише з незначною кількістю помилок	зараховано	90 – 100
B	**Дуже добре** – вище середнього рівня з кількома помилками		80 – 89
C	**Добре** – у цілому правильна робота з певною кількістю незначних помилок		75 – 79
D	**Задовільно** – непогано, але зі значною кількістю недоліків		70 – 74
E	**Достатньо** – виконання задовольняє мінімальні критерії		60 – 69
FX	**Незадовільно** – потрібно попрацювати перед тим, як перескладати	не зараховано	35 – 59
F	**Незадовільно** – необхідна серйозна подальша робота, обов'язковий повторний курс		0 – 34