Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут права і соціальних технологій
Кафедра кримінального права та правосуддя

РОБОЧА ПРОГРАМА

Запобігання кіберзлочинам

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Коломієць Н.В.
(підпис) (прізвище та ініціали)
«01» вересня 2025р.

Розробник (-и): Толкач А.М., ст. викладач кафедри _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедра кримінального права та правосуддя

Протокол від «01» вересня 2025р. №10
Узгоджено з гарантом освітньої програми: _____ Коломієць Н.В.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Вибіркова*
Мова викладання	українська
Рік навчання та семестр	4 рік, 7 семестр Освітня програма «Кримінальна юстиція (Суд. Прокуратура. Адвокатура)»
Викладач (-і)	Толкач А.М., ст. викладач кафедри
Профайл викладача (-ів)	https://kriminal.stu.cn.ua/
Контакти викладача	angela-0044@stu.cn.ua

2. Анотація курсу. Дисципліна «Запобігання кіберзлочинам» займає важливе місце у програмі навчання бакалаврів права за ОПП «Кримінальна юстиція (Суд. Прокуратура. Адвокатура)», спеціальності 081 – «Право». Розкривається 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.

Успішне засвоєння дисципліни «Запобігання кіберзлочинам» дозволяє бакалавру права розширити коло застосування набутих раніше знань та практичних навичок для вирішення різноманітних правових ситуацій у сфері міжнародних відносин, що мають міждержавний характер.

Програма навчальної дисципліни складається з таких модулів:

1) Модуль 1. Формування та реалізація державної політики в сфері кіберзахисту.

Основні цілa, напрями та принципи державної політики у сфері кібербезпеки. Правові основи забезпечення кібербезпеки України. Об'єкти кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. Передумови та чинники кіберзагроз. Заходи забезпечення кібербезпеки. Стратегія, законодавство, напрямки сучасної політики у сфері кібербезпеки в Україні та зарубіжних країнах. Концепція розвитку науки щодо запобігання кіберзлочинності в Україні на початку XXI століття.

2) Модуль 2. Поняття кіберзлочину та механізми його запобігання.

Поняття і визначення кіберзлочину. Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності. Запобігання кіберзлочинам як міжгалузева дисципліна. Класифікація кіберзлочинів. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі. Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення. Кількісно-якісне вимірювання кіберзлочинності. Рівень кіберзлочинності. Структура кіберзлочинності. Кримінально-правові ознаки структури кіберзлочинності. Кримінологічні ознаки структури кіберзлочинності. Динаміка кіберзлочинності. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно рольові властивості особистості кіберзлочинця. Соціальне і біологічне в особистості кіберзлочинця, їх співвідношення. Типологія кіберзлочинців. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології. Поняття Об'єкти запобігання кіберзлочинності. Суб'єкти запобігання кіберзлочинності та основні напрями їх діяльності.

3) Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.

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. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Причини та умови злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. 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)

3. Мета та цілі курсу. Метою курсу «Запобігання кіберзлочинам» є 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.

Завдання, які вирішуються в процесі вивчення курсу:

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

- опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки;

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

- 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.

Під час вивчення курсу здобувач вищої освіти має набути або розширити наступні загальні та спеціальні компетентності, передбачені освітньою програмою:

ЗК 2. Здатність застосувати знання у практичних ситуаціях.

ЗК 3. Знання та розуміння предметної області та розуміння професійної діяльності.

СК 11. Здатність визначати належні та прийнятні для юридичного аналізу факти.

СК 13. Здатність до критичного та системного аналізу правових явищ.

4. Результати навчання. Під час вивчення курсу здобувач вищої освіти має досягти або вдосконалити наступні програмні результати навчання, передбачені освітньою програмою:

РН 6. Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.

РН 19. Пояснювати природу та зміст основних правових явищ і процесів.

РН 20. Виокремлювати і аналізувати юридично значущі факти і робити обґрунтовані правові висновки.

5. Обсяг курсу. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи.

Вид заняття	Загальна кількість годин
Лекції	16
Лабораторні заняття	14
Самостійна робота	60
Індивідуальне завдання	контрольна робота
Всього кредитів – *вказати кількість кредитів*	3

Формами проведення занять є лекційні та практичні (семінарські) заняття, самостійна робота, виконання контрольної роботи. Проведення занять відбувається на парах згідно розкладу та за допомогою платформи дистанційного навчання «MOODLE».

6. Тематика курсу.

Тематика лекційних занять

Тема 1. Поняття кібербезпеки, її основні категорії

Поняття кібербезпеки. Основні категорії кібербезпеки. Об'єкти системи протидії кіберзлочинності. Суб'єкти протидії кіберзлочинності. Надійність пароля як інструмент забезпечення кібербезпеки

Тема 2. Правові основи забезпечення кібербезпеки України

Законодавство України про забезпечення кібербезпеки. Характеристика Закону України «Правові основи забезпечення кібербезпеки України». Стратегія кібербезпеки України. Конвенція про кіберзлочинність

Тема 3. Поняття і визначення кіберзлочину. Показники кіберзлочинності

Поняття кіберзлочинності та кіберзлочинів. Причини та умови кіберзлочинності. Вимірювання рівня кіберзлочинності. Структура кіберзлочинності. Класифікація кіберзлочинів

Тема 4. Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця. Детермінація кіберзлочинності

Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця. Детермінація кіберзлочинності.Зміст поняття «кіберзлочинець» та його характеристика. Характеристика осіб, які вчиняють кіберзлочини. Поняття особи кіберзлочинця. Структура особистості кіберзлочинця (соціально-демографічні ознаки та морально-психологічні якості). Типологія кіберзлочинності. Наукове і практичне значення вивчення особистості кіберзлочинців

Тема 5. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів

Запобігання кіберзлочинності: поняття, зміст, значення. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності і окремих злочинів. Об'єкти запобігання кіберзлочинності. Суб'єкти запобігання кіберзлочинності та основні напрями їх діяльності.

Тема 6. 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

Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Причини та умови кримінальних правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

Тема 7. 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) . Особистість кібершахрая, основні риси. Причини і умови 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). Запобігання кіберзлочинам, пов’язаним з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо).

Тема 8. 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. Особистість кіберзлочинця, основні риси. Причини і умови кіберзлочинів, пов’язаних з контентом (змістом даних), розміщених у комп’ютерних мережах (зокрема злочини, пов’язані з дитячою порнографією). Характеристика кіберзлочинів, пов’язаних з порушенням авторського права і суміжних прав. Причини та умови кіберзлочинів пов’язаних з порушенням авторського права і суміжних прав. Запобігання кіберзлочинам пов’язаних з порушенням авторського права і суміжних прав. Поняття та кримінологічна характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп’ютерних мереж). Хуліганство у віртуальній сфері. Запобігання кіберзлочинам проти громадського порядку та моральності. Кіберзлочинність у сфері економіки. Характеристика кіберзлочинів у сфері економіки. Особистість кіберзлочинця, основні риси. Захист об’єктів критичної інфраструктури. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки. Характеристика кіберзлочинів у сфері обігу наркотичних засобів. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів. Запобігання кіберзлочинам у сфері обігу наркотичних засобів. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності. Характеристика організованої кіберзлочинності. Причини та умови організованої злочинності. Запобігання організованій злочинності. Міжнародне співробітництво у сфері запобігання організованій злочинності. Корупція у віртуальній сфері. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів. Характеристика корупційної кіберзлочинності. Причини та умови корупційної злочинності. Запобігання корупційній злочинності. Характеристика злочинності неповнолітніх у віртуальній сфері. Особистість неповнолітнього кіберзлочинця, основні риси. Причини та умови кіберзлочинності неповнолітніх. Запобігання кіберзлочинності неповнолітніх.

Тематика семінарських занять

1. Поняття кібербезпеки, її основні категорії. Правові основи забезпечення кібербезпеки України
2. Поняття і визначення кіберзлочину. Показники кіберзлочинності
3. Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця. Детермінація кіберзлочинності
4. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів
5. 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

6. 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).

7. Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією) та інших кіберзлочинів

Тематика самостійної роботи

Самостійне опрацювання окремих питань в межах тем:

Характеристика кіберзлочинів у сфері економіки. Особистість кіберзлочинця, основні риси. Захист об'єктів критичної інфраструктури. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки. Характеристика кіберзлочинів у сфері обігу наркотичних засобів. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів. Запобігання 10кіберзлочинам у сфері обігу наркотичних засобів. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності. Характеристика організованої кіберзлочинності. Причини та умови організованої злочинності. Запобігання організованій злочинності. Міжнародне співробітництво у сфері запобігання організованій злочинності. Корупція у віртуальній сфері. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів. Характеристика корупційної кіберзлочинності. Причини та умови корупційної злочинності. Запобігання корупційній злочинності. Характеристика злочинності неповнолітніх у віртуальній сфері. Особистість неповнолітнього кіберзлочинця, основні риси. Причини та умови кіберзлочинності неповнолітніх. Запобігання кіберзлочинності неповнолітніх.

7. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання знань ЗВО здійснюється за 100-бальною шкалою з подальшим переведенням у національну шкалу (шкалу Університету) та шкалу ECTS, відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету "Чернігівська політехніка"» (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-potochne-ta-pidsumkove-oczinyuvannya-znan-zdobuvachiv-vo.pdf). Система оцінювання знань з навчальної дисципліни «Запобігання кіберзлочинам» включає *поточний та семестровий контроль знань.* У 7 семестрі ЗВО може набрати до 70% підсумкової оцінки за виконання протягом семестру всіх видів робіт і до 30% підсумкової оцінки на диференційованому заліку. Якщо здобувач вищої освіти виконав всі види робіт протягом семестру, то він, за

	бажанням, може залишити набрану кількість балів як підсумкову оцінку і не складати залік. Повторне складання диференційованого заліку з метою підвищення позитивної оцінки не дозволяється, але у виняткових випадках за погодженням з деканом факультету такий дозвіл може дати ректор Університету. Поточний контроль проводиться шляхом спілкування із здобувачами вищої освіти під час лекцій, семінарських занять, усного та письмового опитувань здобувачів вищої освіти, оцінювання результатів неформальної освіти, оцінювання реферування наукової роботи, виконання самостійної роботи та написання однієї контрольної роботи. Семестровий *контроль по закінченню 7 семестру проводиться у формі* ***диференційованого заліку*** відповідно до графіку навчального процесу згідно затвердженого розкладу. Для складання заліку існують білети. Білети складаються з двох питань *(кожне питання оцінюється максимум у 15 балів)*. У **13-15 балів** оцінюється відповідь на питання, яка є повною, її зміст відповідає сутності поставленого питання, (допускаючи при цьому 1-2 незначні помилки). **10-12 балів** - відповідь правильна, послідовна, логічна, але ЗВО допускає у викладі окремі незначні пропуски фактичного матеріалу; **6-9 бали** ЗВО володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, нечітко, а інколи й невірно формулює основні теоретичні положення; **1-5 бали** ЗВО виявляє незнання більшої частини фактичного матеріалу; відповідь не розкриває поставлених запитань чи завдань; допускає грубі помилки; **0 балів** – ставиться коли відповідь на питання є повністю неправильною. Оцінювання успішності ЗВО під час семестрового контролю вноситься у відомість успішності та навчальну картку здобувача вищої освіти в автоматизованій системі управління – АСУ «ВНЗ».
Семінарські (практичні) заняття	**Усне опитування** - включає в себе опитування за будь-яким питанням, винесеним на семінарське заняття (за вибором викладача), відповідь на питання інших ЗВО, відповідь на питання для повторення (з тем, що було вивчено раніше), відповіді на контрольні питання з теми семінарського заняття. Максимальна кількість балів може бути виставлена ЗВО, підготовленим до відповідей на усі питання теми, включаючи питання винесені на самостійне опрацювання. Оцінюючи відповідь, викладач керується такими критеріями, як: **5 балів** - повне, послідовне та

	обґрунтоване викладення матеріалу. Відповідь свідчить про глибоке розуміння питання та його зв'язок з іншими темами та питаннями. **4 бали** - ЗВО дає правильний, повний виклад змісту підручника і матеріалу, поданого викладачем, але на додаткові контрольні питання, які ставить викладач відповідає не чітко. **3 бали** - ЗВО виявляє знання і розуміння основного навчального матеріалу, що розглядається, але під час відповіді допускає суттєві помилки і усвідомлює їх тільки після повторної вказівки викладача. Викладає матеріал не послідовно. Відповіді на уточнюючі запитання дає не одразу, не впевнено та не чітко. На додаткові питання викладача не відповідає, або відповідає дуже поверхово. **2 бали –** ЗВО у відповіді припускається грубих помилок і не виправляє ці помилки навіть при вказівці на них викладача; поверхово орієнтується в питанні та темі, яка обговорюється на семінарському занятті. **1 бал** – ЗВО намагається відтворити зміст матеріалу, однак взагалі не розуміє його змісту, зв'язків терміно-понять та їх місця питанні, що вивчається. **0 балів** отримує ЗВО, який відмовляється відповідати на запитання. **Реферування наукової літератури** полягає у самостійному опрацюванні ЗВО наукової літератури (як правило наукової статті), критичному огляді та короткому переказі її змісту, а також наведення найважливіших висновків. **Оцінювання виконання реферування, індивідуальної роботи здійснюється на основі наступних критеріїв:** оформлення роботи, уміння самостійно працювати з науковими джерелами та нормативно-правовими актами, чітко визначати актуальність досліджуваного питання, на основі проведеного аналізу формулювати власну позицію: - *4-5 балів* – матеріал викладений логічно і повно, результати дослідження мають практичну і теоретичну цінність, висновки аргументовані і обґрунтовані; - *4-3 бали* – матеріал викладений логічно і повно, результати дослідження мають практичну і теоретичну цінність, висновки недостатньо аргументовані і обґрунтовані; - *3-2 бал* – матеріал викладений недостатньо повно, індивідуальна робота не достатньо аргументована, обґрунтована та/або не стосується усіх поставлених завдань; - *1-0 балів* – викладений матеріал неповний, індивідуальна робота не є структурованою, висновки поверхневі або відсутні. Максимальна кількість балів – 5 бали. Такий вид роботи кожен студент може виконати не більше одного разу за кожен змістовий модуль.
Умови допуску до підсумкового контролю	У випадку, якщо ЗВО протягом семестру не виконав у повному обсязі передбачених робочою програмою

	навчальної дисципліни всіх видів навчальної роботи, має більше 30% пропусків навчальних занять (без поважних причин) від загального обсягу аудиторних годин відповідної навчальної дисципліни або не набрав мінімально необхідну кількість балів (тобто кількість балів, яка сумарно з максимально можливою кількістю балів, які ЗВО може отримати під час семестрового контролю не дозволить отримати підсумкову оцінку «задовільно – Е, 60 балів»), *(4 семестр – 30 балів), то* він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість. На ліквідацію академічної заборгованості виноситься весь обсяг теоретичного матеріалу, що передбачений робочою програмою навчальної дисципліни «Запобігання кіберзлочинам». Академічна заборгованість повинна бути ліквідована до атестації здобувача вищої освіти, а у випадку коли заборгованість виникла з дисципліни, знання, уміння та навички з якої, відповідно до структурно-логічної схеми підготовки фахівця, потрібні для вивчення навчальних дисциплін наступного семестру, то така заборгованість повинна бути ліквідована до початку нового семестру. Академічна заборгованість ліквідується здобувачами вищої освіти протягом наступних семестрів згідно з розкладами ліквідації академзаборгованості, що затверджуються деканом факультету за поданням відповідних кафедр. Результати ліквідації академзаборгованості відображаються в ліквідаційній відомості успішності.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**лькістьбалів**
1	Робота на практичному занятті	0…50
2	Самостійне опрацювання теми	0…5
3	Виконання тестових завдань	0…5
Усього поточний і проміжний модульний контроль		**0…60**
Семестровий контроль (Екзамен)		**0…40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**

		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

8. Політики курсу. У випадку, якщо ЗВО протягом семестру не виконав у повному обсязі передбачених робочою програмою навчальної дисципліни всіх видів навчальної роботи, має більше 30% пропусків навчальних занять (без поважних причин) від загального обсягу аудиторних годин відповідної навчальної дисципліни або не набрав мінімально необхідну кількість балів (тобто кількість балів, яка сумарно з максимально можливою кількістю балів, які ЗВО може отримати під час семестрового контролю не дозволить отримати підсумкову оцінку «задовільно – Е, 60 балів»*), то* він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти Національного університету «Чернігівська політехніка». Недопустимі пропуски та запізнення на заняття; користування мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування; недотримання строків виконання навчально-наукових завдань тощо. За об'єктивних причин (наприклад, карантин, хвороба, міжнародне стажування) навчання може відбуватись дистанційно за погодженням із деканатом та викладачем, що читає курс.

Загальні засади освітнього процесу в НУ «Чернігівська політехніка» закріплені Положенням про організацію освітнього процесу в Національному університеті «Чернігівська політехніка, затв. Вченою радою від 31.08.2020 https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf та Положенням про дистанційне навчання в Національному університеті «Чернігівська політехніка», затв. Вченою радою 31.08.2020 https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-dystanczijne-navchannya.pdf

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 15 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, тощо.

Політика академічної доброчесності

Політика дотримання академічної доброчесності ґрунтується на Кодексі академічної доброчесності Національного університету "Чернігівська політехніка" https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/kodeks-akademichnoyi-dobrochesnosti.pdf .

Дотримання академічної доброчесності здобувачами освіти передбачає: - самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); - посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; - дотримання норм законодавства про авторське право і суміжні права; - надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушення академічної доброчесності здобувачами вищої освіти можуть мати наслідки: - повторне проходження оцінювання (контрольна робота, залік тощо); - повторне проходження відповідного освітнього компонента освітньої програми; - відрахування з Університету; - позбавлення академічної стипендії.

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

9. Рекомендована література.

1. Віктимологія : навч. посібник/ В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін. ; за ред. В.В. Голіни і Б.М. Головкіна. Харків : Право, 2017. 343 с.

2. Захист прав, приватності та безпеки людини в інформаційну епоху. Монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

3. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи Тарасюк А. В. : монографія. Київ; Одеса : Фенікс, 2020. 404 с.

4. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. Харків : Право, 2020. 373 с.

5. Muravska Yuliia. Theoretical and conceptual approaches to defining the concept and forms of economic intelligence.in the Ukrainian scientific practice. Osteuropa-Recht. 2022. Vol. 4. P. 476-485.

Інтернет-джерела.

1. Посилання на сторінку дисципліни в системі дистанційного навчання moodle. URL: https://eln.stu.cn.ua/enrol/index.php?id=6880

2. Офіційний сайт Верховної Ради України. URL: https://www.rada.gov.ua/

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

4. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації

України. URL: https://cip.gov.ua/
5. Єдиний державний реєстр судових рішень URL: http://www.reyestr.court.gov.ua/