СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

Основи виявлення та розслідування кіберзлочинів

спеціальність	**не обмежено**	**обов'язковість дисципліни**	**вибіркова**
освітня програма	**не обмежено**	**факультет**	**навчально-науковий інститут «Кіберпорт»**
освітній рівень	**не обмежено**	**кафедра**	**інформаційних технологій, кібернетики та захисту інформації**

ВИКЛАДАЧ

ЧАЛИЙ ІГОР ВІЛЬОВИЧ

Вища освіта – спеціальність „Динаміка та міцність машин ”
Науковий ступень - кандидат технічних наук 05.20.01
Вчене звання - доцент кафедри кібернетики та інформаційних технологій
Досвід роботи – більше 42 років
Показники професійної активності з тематики курсу:

- автор більше 10 методичних розробок;
- співавтор 2 навчальних посібників;
- співавтор 2 тематичних публікацій (1 Scopus);
- учасник наукових і методичних конференцій.

телефон	**0503032421**	**електронна пошта**	**ivchaly@gmail.com**	**дистанційна підтримка**	**Moodle**

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

Мета	**отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних, а також формування вмінь брати участь у проведенні первинних криміналістичних розслідувань порушень кібербезпеки.**
Формат	**лекції, практичні заняття, самостійна робота, індивідуальні завдання**
Деталізація результатів навчання і форм їх контролю	• **ознайомлення з базовими поняттями і значенням криміналістики / лекції, практичні завдання;** • **ознайомлення з криміналістичними характеристиками злочинів, вчинених у кіберпросторі / лекції, практичні завдання;** • **розгляд методичних основ розслідування кіберзлочинів / лекції, практичні завдання;** • **вивчення основних організаційних засад виявлення та кримінального провадження щодо кіберзлочинів / лекції, практичні завдання, індивідуальні завдання;** • **огляд спеціальних знань, що використовуються під час розслідування кіберзлочинів / індивідуальні, практичні завдання, самостійна робота;** • **вивчення основних інструментів, що використовуються під час розслідування кіберзлочинів / лекції, практичні завдання;** • **аналіз можливостей порталу "Лабораторія комп'ютерної криміналістики" для вивчення дисципліни./ індивідуальні, практичні завдання, самостійна робота.**
Обсяг і форми контролю	**3 кредити ECTS (90 годин): 12 годин лекції, 18 годин лабораторно-практичні; модульний контроль (2 модулі); підсумковий контроль – диференційований залік.**
Вимоги викладача	**вчасне виконання завдань, активність, самостійна робота.**
Умови зарахування	**вільне зарахування**

ВІДПОВІДНІСТЬ СТАНДАРТУ ОСВІТИ І ОСВІТНІЙ ПРОГРАМІ

Компетенції	**Здатність застосовувати основи інформаційної безпеки у фаховій та навчальній діяльності.**	**Програмні результати навчання**	**Застосовувати знання з основ інформаційної безпеки у навчанні та повсякденній роботі за фахом.**

СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)					
Модуль 1. ОСНОВИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ.					
Лекція 1.	**Предмет та значення дисципліни. Поняття і значення криміналістики. Кіберпростір та злочини як об'єкт криміналістичного дослідження.**	**Лабораторно-практичне заняття 1 (ЛПЗ 1)**	**Огляд джерел Інтернет стосовно цифрової криміналістики. Термінологія OSINT.**	**Самостійна робота**	**Поглиблений огляд джерел Інтернет стосовно цифрової криміналістики. Криміналістичні інформаційні системи. Експертна система для аналізу кримінального законодавства. Аналіз можливостей порталу " Компанія ЕПОС" для вивчення дисципліни. Розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, що пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. Безкоштовні Інструменти кібербезпеки SANS https://www.sans.org/tools/?focus-area=digital-forensics Самостійне доопрацювання матеріалів змістовного модуля 1.**
Лекція 2.	**Криміналістична характеристика злочинів, вчинених у кіберпросторі. Методичні основи розслідування кіберзлочинів. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами.**	**ЛПЗ 2**	**Методичні основи розслідування кіберзлочинів. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами.**		
Лекція 3.	**Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів. Суб'єкти взаємодії зі слідчим під час розслідування злочинів, вчинених у кіберпросторі.**	**ЛПЗ 3**	**Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.**		
.		**ЛПЗ 4**	**Правила безпечного опрацювання даних.**		
		ЛПЗ 5	**Аналіз можливостей порталу "Лабораторія комп'ютерної криміналістики" для вивчення дисципліни.**		
Модуль 2. РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ.					
Лекція 4.	**Використання спеціальних знань під час розслідування кіберзлочинів.**	**ЛПЗ 6**	**Засоби блокування запису.**	**Самостійна робота**	**Самостійне проходження з отриманням сертифікату освітнього ресурсу порталу «Cybrary, Inc» - " Incident Response and Advanced Forensics — Реагування на інциденти та вдосконалена криміналістика ". Самостійне проходження з отриманням сертифікату освітнього ресурсу порталу «Cybrary, Inc» - " Computer Hacking & Forensics — Комп'ютерний злом і криміналістика ". Безкоштовно пройти тест з основ**
Лекція 5.	**Організаційно-тактичні основи розслідування кіберзлочинів.**	**ЛПЗ 7**	**Організаційно-тактичні основи розслідування кіберзлочинів.**		
Лекція 6.	**Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі.**	**ЛПЗ 8**	**Провідні світові розробники засобів розслідування IT-інцидентів: ICS, Decision Group, Guidance Software, Cellebrite, Tableau, eDEC, iStorage, Barracuda Networks, X-Ways, Rapid7 та інші.**		
		ЛПЗ 9	**Самостійне проходження з**		

			отриманням сертифікату освітнього ресурсу порталу «Cybrary, Inc» - " Everyday Digital Forensics — Щоденна цифрова криміналістика ".		комп'ютерної криміналістики https://www.skillset.com/skills/computer-forensics-fundamentals Каталог засобів і методів комп'ютерної криміналістики https://toolcatalog.nist.gov/index.php Самостійне доопрацювання матеріалів змістовного модуля 2.

ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

Література

1. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.
2. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. – Одеса :ТЕС, 2020. – 372 с.
3. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2016. 449 с.
4. Якименко І.З. Конспект лекцій з дисципліни Цифрова криміналістика Тернопіль - 2020. – 109 с.
5. Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2023. – 388 с.
6. Sachowski J. Implementing Digital Forensic Readiness: From Reactive to Proactive Process Syngress. — 375 p.
7. Федотов Н.Н. Форензика – компьютерная криминалистика –М.: Юридический Мир, 2007. – 432 с.

Методичне забезпечення

1. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.]; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.
2. Електронні докази. Обшук / [О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін.]. Харків: Фактор, 2020. Ч. 1. 80 с.
3. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рекомендації / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.
4. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рекомендації / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.
5. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів [Текст] : метод. рек. / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. – К., 2016. – 55 с.
6. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту [Текст] : метод. рек. / [Стрільців О. М., Крижна В. В., Максименко О. В. та ін.] ; за заг. ред. Ю. Ю. Орлова. – К. : Нац. акад. внутр. справ, 2014. – 80 с.

СИСТЕМА ОЦІНЮВАННЯ (електронне посилання на положення)

СИСТЕМА		БАЛИ	ДІЯЛЬНІСТЬ, ЩО ОЦІНЮЄТЬСЯ
Підсумкове оцінювання	100 бальна ECTS (стандартна)	до 50	50% від усередненої оцінки за модулі
		до 50	підсумкове тестування
Модульне оцінювання	100 бальна сумарна	до 50	відповіді на тестові питання
		до 20	усні відповіді на лабораторно-практичних заняттях
		до 30	результат засвоєння блоку самостійної роботи

НОРМИ АКАДЕМІЧНОЇ ЕТИКИ ТА ДОБРОЧЕСНОСТІ

Всі учасники освітнього процесу (в тому числі здобувачі освіти) повинні дотримуватися кодексу академічної доброчесності та вимог, які прописані у положенні «Про академічну доброчесність учасників освітнього процесу ДБТУ»: виявляти дисциплінованість, вихованість, поважати гідність один одного, проявляти доброзичливість, чесність, відповідальність.