СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Цифрова криміналістика
Мова викладання	Українська
Викладач (-і)	М.Є. Шелест професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
Профайл викладача (-ів)	0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. Анотація курсу – в даному курсі розглядаються загрози для інформаційних систем, вивчаються їх вразливості, формуються уміння проводити розслідування комп'ютерних інцидентів, виявляти обставини комп'ютерних злочинів за допомогою сучасних засобів. Тематика курсу – сучасні інформаційні технології.

2. Мета та цілі курсу – формування науково-професійного світогляду магістра спеціальності *Кібербезпека* в області безпеки інформаційних і комунікаційних систем, уміння вирішувати задачі адміністрування мереж та систем, проводити розслідування комп'ютерних інцидентів, виявляти обставини комп'ютерних злочинів за допомогою сучасних засобів.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

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

3. Результати навчання

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 2. Планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

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

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 5. Реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 6. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою.

Після курсу здобувач вищої освіти отримає наступні навички:

1. проводити розслідування комп'ютерних інцидентів;
2. виявляти обставини комп'ютерних злочинів за допомогою сучасних засобів;
3. виявляти вразливості периметра комп’ютерної мережі.
4. захищати інформаційні системи від кібератак.

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

Вид заняття	**Загальна к-сть годин**
лекції	22
практичні заняття	18
самостійна робота, контрольна робота	110

5. Пререквізити – для вивчення даної дисципліни бажаним є прослуховування курсу «Комп’ютерні мережі».

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	З дисципліни ЗВО може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на заліку.
Вимоги до реферату	Відповідність умовам завдання – до 5 балів; посилання на першоджерела – до 5 балів; своєчасність здачі – до 5 балів. Захист реферату: самостійність виконання (відповіді на запитання) – до 5 балів.
Умови допуску до підсумкового контролю	У випадку, якщо ЗВО протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (20), він не допускається до складання екзамену під час сесії, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань ЗВО ЧНТУ».

7. Політики курсу - Виконання та особистий захист усіх практичних робіт, зазначених у робочій навчальній програмі з дисципліни, є обов'язковим. Поточний контроль проводиться шляхом спілкування із ЗВО під час лекцій та консультацій та опитувань ЗВО під час захисту практичних робіт.

8. Рекомендована література

1. Закон України від 7 вересня 2005 р. "Про ратифікацію Конвенції про кіберзлочинність"http://zakon.rada.gov.ua/.
2. National Institute of Justice. Special Report. Test Results for Hardware Write Block Device: FastBloc IDE (Firmware Version 16), 2006.
3. National Institute of Justice. Special Report. Test Results for Hardware Write Block Device: ICS ImageMasster DriveLock IDE (Firmware Version 17), 2006.
4. National Institute of Standards and Technology. Hardware Write Blocker (HWB) Assertions and Test Plan, 2005.
5. AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS), Rev. 6a, 2008.
6. James R. Lyle. A strategy for testing hardware write block devices. Digital Investigation, 3S (2006) S3–S9.
7. Аппаратный блокиратор записи EPOS WriteProtector. Руководство пользователя. ООО «ЕПОС», 2011.
8. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009.
9. Домарев В.В. Безопасность информационных технологий. – М.:DS, 2004.
10. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003.
11. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: ЮНИОР, 2003.