СКОРОЧЕНИЙ ОПИС ДИСЦИПЛІНИ

ОСНОВИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

(назва дисципліни)

Обсяг дисципліни – 3 кредити ЄКТС, лекцій – 18 год., практичних занять – 8 год., лабораторних занять – 12 год., форма контролю – іспит комбінований.

Дисципліна вивчається на першому рівні вищої освіти (освітній ступень - бакалавр). Надаються теоретичні та практичні аспекти формування у здобувачів компетенцій щодо розслідування різних аспектів кіберзлочинів, аналізу різних складних інформаційних систем, у тому числі операційних систем, мережі, файлової системи і аналізу пам'яті. Наявність такого роду досвід допоможе студентам у їх майбутньому житті не тільки, якщо вони працюють в цифровій судової області (цифровій криміналістиці), а й для виявлення слідів від ненавмисного пошкодження інформації для їх подальшого аналізу з боку фахівців-криміналістів.

1. Перелік тем дисципліни.

Змістовий модуль 1.

1. Основи цифрової криміналістики. Вступ. Основні аспекти цифрової криміналістики. Структура курсу. Попередні знання. Результати. Основи цифрової експертизи. Значення цифрової криміналістики. Історія. Стандартні операційні процедури. Посилання / література для самоосвіти.
2. Правові аспекти цифрової криміналістики. Стандарти для ідентифікації, збору, придбання і збереження цифрових доказів (наприклад, ISO / IEC 27037). Опис інструменту з коротким оглядом: TSK, xmount, guymager, EWF-інструментів і т.д.

Змістовий модуль 2.

2. Цифрова криміналістика файлових систем

Тема 2.1. Збір даних. 1. Створення образу для цифрової криміналістичної експертизи. Опис інструментів. Команди Linux 2. Формати зображень: dd (Формат RAW); EWF (докази стислого файлу) 3. Хешування; докази контролю цілісності; MD5, SHA1, SHA256 (проблема хеш-колізії)

Тема 2.2. Розмітка. 1. Особливості фізичних та логічних томів. Інструменти для аналізу розділів: MBR, GPT. 2. Огляд RAID.

Тема 2.3. Файлова система Windows. FAT. Основні особливості FAT. Інструменти для FAT аналізу.

Тема 2.4. Файлова система Windows. NTFS. Основні особливості NTFS (резидентів / нерезидентів, атрибути і т.д.) 2. Інструменти для NTFS аналізу.

Тема 2.5. Файлова система Linux. Основні особливості Ext (superblocks, inodes, groupdescriptor тощо). Засоби для NTFS аналізу.

Тема 2.6. Файлова система Mac операційної системи. Основні особливості HFS і HFS + (каталог файлів, дозволи, атрибути і т.д.). Інструменти для аналізу HFS.

Змістовий модуль 3.

3.Цифрова криміналістика операційних систем

Тема 3.1. Аналіз артефактів Windows. 1. Журнали Windows 2. Prefetch 3. Інструменти для аналізу Windows, артефактів (Libevent, libev TX, regripper, і т.д.). 4. Реєстр. 5. VSS. 6. Інструменти для аналізу Windows, артефактів (libvshadow, regripper, і т.д.).

Тема 3.2. Аналіз internet додатків Windows. 1. Browsers. .2. Messengers. 3. P2P артефакти. 4. Засоби для аналізу додатків Windows (sql lite-browser, etc).

Тема 3.3. Аналіз Windows додатків. 1. Аналіз Files metadata. 2. Encryption (bitlockers). 3.Засоби для аналізу артефактів додатків Windows.

Тема 3.4. Аналіз артефактів Linux.1. Конфігурація. 2.Аналіз Log. 3. History / User homefolder.

Тема 3.5. Аналіз артефактів Mac OS. 1. Plist. 2. Аналіз Log. 3. User library.

Змістовний модуль 4.

4. Інші джерела цифрової криміналістики.

Тема 4.1. Мережна криміналістика.1. Sniffing Network traffic. 2.Аналіз прикладного рівня. 3. Засоби для мережевої криміналістики. (Wireshark, Ettercap, та інші).

Тема 4.2. Жива (Live) криміналістика. 1. Як впоратися з живих машин 2. Летючі дані функції і джерела 3. Придбання летючих даних (Windows, Linux, Mac OS).

Тема 4.3. SSD криміналістика. 1. Особливості збору даних SSD. 2. Інструменти для збору даних SSD

Тема 4.4. Аналіз памяті. 1. Основи аналізу пам'яті. 2. Волатильність 3. Аналіз RAM- dump.

2. Вимоги до попередньо набутих компетентностей (за потребою).

Попередньо мають бути вивчені дисципліни: Безпека інформації в інформаційно-комунікаційних системах. Введення в спеціальність. Нормативно-правове забезпечення інформаційної безпеки. Основи технічного захисту інформації. Безпека та аудит безпроводових мереж. Основи захисту сучасних операційних систем.

3. Перелік компетентностей, яких набуде здобувач вищої освіти після опанування даної дисципліни.

1. Здатність застосовувати знання у практичних ситуаціях.
2. Знання та розуміння предметної області та розуміння професії.
3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
4. Здатність до пошуку, оброблення та аналізу інформації
5. Здатність реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
6. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
7. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленою політикою інформаційної та/або кібербезпеки

4. Перелік результатів навчання, яких набуде здобувач вищої освіти після опанування даної дисципліни.

- 1.Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- 2. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
- 3. 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.
- 4. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
- 5. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
- 6. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
- 7. Вміння написання звіту щодо судової експертизи у відповідності з існуючими шаблонами.
- 8. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- 9.Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
- 10. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
- 11. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

5. Кафедра, що пропонує дисципліну:

Кафедра Інфокоммунікаційної інженерії ім .В.В. Поповського.

6. Провідний викладач:

Снігуров Аркадій Владіславович, доцент кафедри ІКІ ім. В.В. Поповського, кандидат технічних наук, доцент.