МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М.В. Афанасьєв

ЦИФРОВА КРИМІНАЛІСТИКА
робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**другий (магістерський)**
Освітня програма	**КІБЕРБЕЗПЕКА**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри Кібербезпеки та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробник:
Шматко О.В., к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Навчальна дисципліна "Цифрова криміналістика" є базовою та вивчається згідно з навчальним планом підготовки фахівців другого освітнього рівня "магістр" спеціальності 125 "Кібербезпека" всіх форм навчання.

Анотація навчальної дисципліни: Дисципліна "Цифрова криміналістика" є базовою навчально дисципліною за спеціальністю “Кібербезпека”. Вона викладається у другому семестрі магістратури в обсязі 120 год.(4 кредита ECTS), зокрема: лекції – 18 год., лабораторні – 12 год., самостійна робота – 90 год, консультації – 4 год. У курсі передбачено два змістових модулі та одна модульна контрольна робота. Завершується дисципліна іспитом.

Предметом навчальної дисципліни є основні поняття та методи цифрової криміналістики, навики збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux.

Метою навчальної є підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також е фахівців з розслідуваннями пов'язаними з кіберзлочинністю.

Головне завдання курсу – освоєння принципів та методів збору криміналістичної цифрової інформації із систем Linux та Windows, проведення статичного аналізу зловмисного програмного забезпечення "Ransomware", використовуючи інструменти та методи цифрової криміналістики.

У результаті вивчення навчальної дисципліни студент повинен **знати**:

- теоретичні основи і сучасні інформаційні технології аналізу та збору криміналістичної цифрової інформації;
- особливості проведення статистичного аналізу зловмисного програмного забезпечення;
- принципи роботи програмного забезпечення з відкритим кодом для збору цифрової криміналістичної інформації;
- сучасний стан і шляхи розвитку цифрової криміналістики;

вміти:

- встановлювати і настроювати програмне забезпечення для збору цифрової криміналістичної інформації;
- виконувати аналіз шкідливих програм;
- застосовувати Windows Live Linux Response;
- самостійно виконувати збір та аналіз цифрової криміналістичної інформації;
- розробляти методи реагування та випадки порушень кібербезпеки;
- застосовувати інструменти цифрової криміналістики та відновлення для організації захисту даних в ОС Windwos, Linux;

Курс	**5**	
Семестр	**2**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**18**
	семінарські, практичні	**-**
	лабораторні	**12**
Самостійна робота		**90**
Форма підсумкового контролю	**іспит**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
Математичні основи криптології	Основи криптографічного захисту

2. Компетентності та результати навчання за дисципліною:

Загальні компетентності	**Результати навчання**
КЗ 1. Здатність застосовувати знання у практичних ситуаціях (Здатність до застосування концептуальних знань та певних знань сучасних досягнень у професійній діяльності)	РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
КЗ 2. Знання та розуміння предметної області та розуміння професії. (Здатність розуміти сутність та соціальну значущість майбутньої професійної діяльності, виявляти стійкий інтерес до неї)	РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки;
КЗ 6. Здатність до пошуку, обробки та аналізу інформації з різних джерел. (Здатність до самостійного пошуку, аналізу, синтезу та використання інформації, необхідної для ефективного розв'язання професійних завдань.)	РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
Фахові компетентності	Результати навчання
КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
КФ 2. Здатність до використання інфор-	РН-16. Здійснювати професійну діяль-

маційних і комунікаційних технологій	ність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи цифрової криміналістики

Тема 1: Введення в цифрову судову експертизу

Що таке цифрова криміналістика? Чому використовується поняття цифрової криміналістики? Яка мета цифровий криміналістики. Обмеження та труднощі застосування цифрової криміналістики.

Тема 2: Основні концепції та методологія цифрової криміналістики

Основи цифрової криміналістики. Збір доказів. Цифрова криміналістична лабораторія. Цифрові криміналістичні інструменти

Тема 3: Основи цифрової криміналістики

Застосування цифрової криміналістики для сімейства операційних систем Windows. Застосування цифрової криміналістики для сімейства операційних систем Linux / Unix. Типи носіїв і форматів даних. Хешування і шифрування даних. Мобільні пристрої та цифрова криміналістика

Тема 4: Цифрова криміналістика

Процес цифрової криміналістики. Принцип причинно-наслідкових зв'язків. Принцип дотримання належної обережності. Докази проти «чуток»

Змістовий модуль 2. Спеціалізоване програмне забезпечення для цифрової криміналістики

Тема 5: Базові методи використання спеціалізованого програмного забезпечення

Необхідність спеціалізованого програмного забезпечення. Огляд рекомендованих програмних комплектів. Рекомендації по використанню певних програмних інструментів для спеціальних завдань.

Тема 6: Обробка цифрової криміналістики в програмному забезпеченні

Аналіз реєстру Windows. Використання Hex-редактора. Отримання та збереження доказів. Імпорт доказів. Пошук і фільтрація

Тема 7: Типові випадки і рекомендації по їх дослідженню

Типові випадок інциденту, пов'язаного з витоком даних. Типовий випадок інциденту з компрометації клієнтського пристрою / системи. Типовий випадок інциденту, причиною якого є шкідливий код.

Тема 8: Звітність і труднощі застосування цифрової криміналістики

Як ефективно вести звітність по роботі цифрового криміналіста. Хмарні технології. Віртуалізація. Мобільні пристрої та принцип BYOD (Bring Your Own Device)

Лабораторні роботи

Тема 5

Лабораторна робота 1. Встановлення та настройка спеціалізованого програмного забезпечення

Тема 6

Лабораторна робота 2. Збір та аналіз цифрової криміналістичної інформаці в ОС Windows

Лабораторна робота 3. Збір та аналіз цифрової криміналістичної інформаці в ОС Linux

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, nf лабораторні роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі письмової контрольної роботи у вигляді тесту (18 тестових питань), як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять проводиться за такими критеріями:

"відмінно" (7-8 балів) - студент бездоганно засвоїв теоретичний матеріал з проблеми пошуку доказів та розслідування інцидентів цифрової криміналістики, демонструє глибокі і всебічні знання методів, інструментальних та програмних засобів збору та аналізу криміналістичної цифрової інформації, основні положення наукових першоджерел та рекомендованої літератури, логічно мислить і будує відповідь, віль-

но використовує набуті теоретичні знання з дослідження та пошуку цифрової криміналістичної інформації, висловлює своє ставлення до тих чи інших проблем, демонструє високий рівень засвоєння практичних навичок із застосування цифрової криміналістики для сімейства операційних систем Windows/Linux/Unix;

- "добре" (4-6 бали) - студент добре засвоїв теоретичний матеріал, володіє основними аспектами з пошуку та аналізу цифрової криміналістичної інформації з першоджерел та рекомендованої літератури, аргументовано викладає його; має практичні навички із застосування цифрової криміналістики для сімейства операційних систем Windows/Linux/Unix, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного;

- "задовільно" (1-3 бали) - студент в основному опанував теоретичними знаннями з пошуку та аналізу цифрової криміналістичної інформації, орієнтується в першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, додаткові питання викликають у студента невпевненість або відсутність стабільних знань; відповідаючи на запитання практичного характеру, пов'язаних із застосуванням цифрової криміналістики для сімейства операційних систем Windows/Linux/Unix, виявляє неточності у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутньою діяльністю;

- "незадовільно" (0 балів) - студент не опанував навчальний матеріал з пошуку та аналізу цифрової криміналістичної інформації, не знає визначень методів пошуку типових випадків порушення конфіденційності даних та рекомендації з їх пошуку, майже не орієнтується в першоджерелах та рекомендованій літературі, практичні навички з обробки цифрової криміналістичної інформації відсутні.

Матеріал для самостійної роботи студентів, який передбачений в темі лабораторного заняття одночасно із аудиторною роботою, оцінюється під час поточного контролю теми на відповідному аудиторному занятті. Оцінювання тем, які виносяться на самостійне опрацювання і не входять до тем аудиторних навчальних занять, контролюються під час підсумкового контролю.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 4 практичних ситуацій (два стереотипних, два діагностичних), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 60 балів, мінімальна кількість, що зараховується, – 35 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрольна робота	Усього
Змістовий модуль	Тема	Тиждень				
Змістовий модуль 1.	1	1	2			2
	2	2	2			2
	3	3				0
		4	2			2
	4	5				0
		6	2			2
Змістовий модуль 2.	5	7				0
		8	2	8	18	28
		9				0
		10	2			2
	6	11		8		8
		12	2			2
	7	13		8		8
		14	2			2
		15				
	8	16	2			2
	Іспит					40
Усього за 2 семестр			18	24	18	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	Зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

1. Маркусь В. О. Криміналістика. Навчальний посібник – К.: Кондор, 2007. – 558 с.

2. 16. Вертузаєв М. С., Голубаєв В. О., Котляревський О. І., Юрченко О. М. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / Під ред. Снігірьова О. П.. –Запоріжжя: ПВКФ «Навел», 1998.

3. Герасимов И.Ф. и Драпкин И.Я. Криминалистика: Учебник для вузов. – М.: Высшая школа, 2000.

4. Шепітько В.Ю. Криміналістика: Підручник для вищих закладів освіти. – К., Ін Юре, 2001, 2004.

5. Baig Mohsin. 50 Reasons for Mastering Cyber Forensics Amazon Digital Services LLC, 2017. — 14 p.

6. Bell Suzanne. Measurement Uncertainty in Forensic Science: A Practical Guide CRC Press, 2016. — 178 p.

7. ЛЕС-Council Computer. Forensics: Investigating Data and Image Files Course Technology, 2009. - 224 pages

8. Sachowski J. Implementing Digital Forensic Readiness: From Reactive to Proactive Process Syngress. — 375 p.

9. Shipley Todd G., Bowker Art. Investigating Internet Crimes Elsevier, 2014.

10. Taroni F., Bozza S., Biedermann A., Garbolino P., Aitken C. Data Analysis in Forensic Science: A Bayesian Decision Perspective N.-Y.: Wiley, 2010.- 390p.

11. Ахмедшин Р.Л., Воронин С.Э. Моделирование в криминалистической деятельности Красноярск: Сибирский институт бизнеса, управления и психологии, 2019. — 281 с.

5.2 Додаткова

12. ISACA. (2015). Overview of Digital Forensics. http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000.

13. Karie, Nickson M. and H. S. Venter (2015). Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, Vol. 60(4), 885–893.

14. Maras Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. Jones and Bartlett.

15. Myers Matthew and Marcus Rogers. (2007). Digital Forensics: Meeting the Challenges of Scientific Evidence. Advances in Digital Forensics: IFIP International Conference on Digital Forensics (pp. 43-50).

16. Roussev Vassil, Candace Quates, and Robert Martel. (2013). Real-time digital forensics and triage. Digital Investigation Vol. 10(2), 158–167.

17. Sammons John. (2017). Digital forensics, 2st edition. Elsevier.

5.3. Інформаційні ресурси в Інтернеті

18. Сайт персональних начальних систем ХНЕУ імені С. Кузнеця за дисципліною «Цифрова криміналістика» https://pns.hneu.edu.ua/course/view.php?id=5683.