Программа учебной дисциплины «Основы компьютерной криминалистики»

Утверждена
Академическим советом ООП
Протокол № от «__»_____20__ г.

Автор	Лазаренко Александр Вячеславович
Число кредитов	3
Контактная работа (час.)	76
Самостоятельная работа (час.)	36
Курс	1
Формат изучения дисциплины	Очный (full time)

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Основные цели освоения дисциплины "Основы компьютерной криминалистики":

- обеспечить студентов базовыми знаниями по компьютерной криминалистике и правовым обеспечениям расследований инцидентов информационной безопасности;
- заложить основы знаний об анализе лог-файлов, алгоритмах расследований инцидентов информационной безопасности, проведении компьютерно-технической экспертизы;
- познакомить студентов с основными программными и аппаратными средствами поиска уликовых данных,
- привить студентам навыки исследовательской работы, предполагающей самостоятельное изучение специфических инструментов и средств, необходимых для решения именно той конкретной проблемы, которая в качестве задачи поставлена перед ним.
-

В результате освоения дисциплины студент должен:

- Знать:
    - Основы компьютерной криминалистики;
    - Правовые нормы расследований инцидентов информационной безопасности;
    - Алгоритмы расследований инцидентов информационной безопасности;
- Уметь:
    - Самостоятельно проводить расследования инцидентов информационной безопасности;
    - Проводить компьютерно-техническую экспертизу;
- Иметь навыки (приобрести опыт):
    - Поиска цифровых следов в компьютерных системах;
    - Фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;
    - Анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы;
    - Документировать противоправные действия злоумышленника.

Изучение данной дисциплины базируется на знаниях студентами математики, основ информатики и алгоритмизации в рамках учебной программы средней школы базового уровня, умении применять математический аппарат при выборе метода решения задачи.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема №1.
Основы компьютерной криминалистики

Краткое содержание:

- Введение в компьютерную криминалистику. Специальность – компьютерный криминалист.
- Особенности современных подходов: Windows криминалистика, криминалистика оперативной памяти, криминалистика мобильных устройств, криминалистика сетевого трафика

Рекомендуемая литература:

1. Michael K Robinson. Digital Forensics Workbook: Hands-on Activities in Digital Forensics
2. John Sammons. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics
3. Cory Altheide, Harlan Carvey. Digital Forensics with Open Source Tools.

Тема №2.
Эволюция целевых атак на банки и online fraud

Краткое содержание:

- Хищения у юридических лиц
- Хищения у физических лиц
- Целенаправленные атаки на банки и финансовые организации
- Технические аспекты атак: методы распространения, мошенничества с банковскими картами, СИМ-картами, подмена платежные поручений и т.д.

Рекомендуемая литература:

1. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for our Connected World
2. Brian Krebs. Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door

Тема №3.
Цифровая гигиена

Краткое содержание:

- Безопасность электронной почты
- Безопасность паролей
- Безопасность мобильный приложений
- Безопасность компьютеров
- Безопасность браузеров
- Безопасность соц. Сетей

Рекомендуемая литература:

1. Kevin Mitnick. Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker

Тема №4.
Построение системы обеспечения ИБ в организации.

Краткое содержание:

- Терминология в области ИБ
- Риск-ориентированный подход к обеспечению ИБ в Организации
- CIS Controls

Рекомендуемая литература:

1. C. Warren Axelrod. Enterprise Information Security and Privacy
2. Gerardus Blokdyk. Enterprise Information Security Architecture: The Ultimate Step-By-Step Guide

Тема №5.
Имитация атак. Взгляд изнутри.

Краткое содержание:

- Эволюция атак группировки Cobalt Strike
- Атака изнутри: инструменты, методы атак, технологии

Рекомендуемая литература:

1. Group-IB. Cobalt: logical attacks on ATMs
2. Mikko Niemala. Anatomy of a cyberattack

Тема №6
Реагирование на инциденты ИБ. Правовая база расследований киберпреступлений

Краткое содержание:

- Построение команды по реагированию на инциденты ИБ
- Дорожная карта при реагировании на инциденты ИБ
- Правовая база расследования киберпреступлений

Рекомендуемая литература:

1. Бачило И. Информационное право

Тема №7
Безопасность криптопроектов

Краткое содержание:

- Криптоиндустрия: новое направление – «старые» угрозы
- Основные участники и риски
- Безопасность криптопроектов

Тема №8
OSINT – поиск информации по открытым источникам

Краткое содержание:

- Поиск с помощью порталов и сайтов организаций
- Поиск с помощью государственных информационных ресурсов
- Поиск с помощью социальных сетей
- Иные источники информации

Рекомендуемая литература:

1. Sudhansu Chauhan. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques.
2. Michael Bazzel. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information

III. ОЦЕНИВАНИЕ

По дисциплине «Основы компьютерной криминалистики» предусмотрены следующие формы контроля:

- текущий контроль
  - домашнее задание
  - тестирования
- итоговый контроль
  - итоговая (экзаменационная) контрольная работа (ЭК), выполняемая письменно или на компьютере, продолжительностью 80 минут.

Распределение контрольных мероприятий по модулям:

	1 нед	**2 нед**	**3 нед**	**4 нед**	**5 нед**	**6 нед**	**7 нед**	**8 нед**
Модуль 3				Т1				Т2
Модуль 4				Т3		ДЗ		ЭК

По всем видам работ выставляется десятибалльная оценка.

Итоговая оценка (ИО) по дисциплине «Основы компьютерной криминалистики» вычисляется по формуле:

ИО = 0,6*(0, 4 * Т + 0,6 * ДЗ) + 0,4*ЭК, где **Т**– оценка, накопленная за тестовые задания третьего и четвертого модулей, ДЗ – оценка за домашнее задание в четвертом модуле, **ЭК** – оценка за итоговую (экзаменационную) контрольную работу.

Т = 0,2* Т1 + 0,5* Т2 + 0,3* Т3

Округление оценок при вычислениях осуществляется до ближайшего целого.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Вопросы для оценки качества освоения дисциплины в рамках текущего контроля студентов:

1. Опишите основные направления деятельности группировки Lazarus
2. Опишите основные направления деятельности группировки Silence
3. Опишите основные направления деятельности группировки Cobalt
4. Опишите основные направления деятельности группировки Moneytaker
5. Вредоносное ПО. Классификация. Жизненный цикл.
6. Darkshops, Malware, Botnets
7. Отмывание денег, Спам, Фишинг, Cybercrime to Cybercrime
8. Threat Intelligence. Существующие платформы.
9. STIX, TAXII Protocols
10. Honeypots. Зачем нужны и как использовать

11. Стратегическая кибербразведка
12. Операционная кибербразведка
13. Назовите имена и фамилии преподавателей, которые вели у вас занятия по ИБ
14. Тактическая кибербразведка
15. OSINT
16. Tor. Как работает
17. Подходы к деанонимизации TOR
18. Что такое «блокчейн» и «криптовалюты»?
19. Основные киберугрозы для участников криптоиндустрии. ICO
20. Основные киберугрозы для участников криптоиндустрии. Смарт-контракты
21. Основные киберугрозы для участников криптоиндустрии. Криптобиржи
22. Основные киберугрозы для участников криптоиндустрии. Криптофонды
23. Основные киберугрозы для участников криптоиндустрии. Майнеры
24. Крупные и успешные кибератаки на проекты блокчейн индустрии
25. Защита интеллектуальной собственности в интернете
26. Мобильная криминалистика. Основные подходы.
27. ИБ результаты 2018 года

V. РЕСУРСЫ

V.1Основная литература

1. Michael K Robinson. Digital Forensics Workbook: Hands-on Activities in Digital Forensics
2. John Sammons. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics
3. Cory Altheide, Harlan Carvey. Digital Forensics with Open Source Tools.
4. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for our Connected World
5. Brian Krebs. Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door
6. Kevin Mitnick. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker
7. C. Warren Axelrod. Enterprise Information Security and Privacy
8. Gerardus Blokdyk. Enterprise Information Security Architecture: The Ultimate Step-By-Step Guide
9. Group-IB. Cobalt: logical attacks on ATMs
10. Mikko Niemala. Anatomy of a cyberattack
11. Бачило И. Информационное право
12. Sudhansu Chauhan. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques.
13. Michael Bazzel. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information

V.2 Дополнительная литература

1. Peter Kim. The Hacker Playbook: Practical Guide To Penetration Testing
2. Chris Sanders. Applied Network Security Monitoring: Collection, Detection, and Analysis
3. Michael Collins. Network Security Through Data Analysis: Building Situational Awareness

V.3Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением.

Учебные аудитории для практических занятий по дисциплине оснащены компьютерами, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.