

**Правительство Российской Федерации**

**Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Национальный исследовательский университет  
«Высшая школа экономики»**

Факультет компьютерных наук  
Департамент программной инженерии

Утверждаю  
Академический руководитель  
образовательной программы  
по направлению 09.03.04  
«Программная инженерия»  
В.В. Шилов

« \_\_\_ » \_\_\_\_\_ 2018 г.

**Программа дисциплины «Основы компьютерной криминалистики»**

для направления 09.03.04 «Программная инженерия»  
подготовки бакалавра

Автор программы:  
**Лазаренко А. В.**

Одобрена на заседании Департамента программной инженерии « \_\_\_ » \_\_\_\_\_ 2018 г.

Руководитель Департамента программной инженерии. \_\_\_\_\_ С.М. Авдошин

Рекомендована Академическим советом образовательной программы  
«Программная инженерия» « \_\_\_ » \_\_\_\_\_ 2018 г.

Москва, 2018

*Настоящая программа не может быть использована другими подразделениями  
университета и другими вузами без разрешения департамента-разработчика программы.*



## **1 Область применения и нормативные ссылки**

Настоящая программа учебной дисциплины "Основы компьютерной криминалистики" устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов направления 09.03.04 «Программная инженерия» подготовки бакалавра, изучающих дисциплину «Основы компьютерной криминалистики».

Программа разработана в соответствии с:

- Образовательным стандартом ФГАОУ ВПО «Национальный исследовательский университет «Высшая школа экономики»;
- Образовательной программой направления 09.03.04 «Программная инженерия» подготовки бакалавра.
- Рабочим планом факультетских дисциплин 2018-2019 уч. года.

## **2 Цели освоения дисциплины**

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 улик 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.

## **3 Компетенции обучающегося, формируемые в результате освоения дисциплины**

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.

## **4 Место дисциплины в структуре образовательной программы**

Настоящая дисциплина является факультативной.

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.

## 5 Тематический план учебной дисциплины

№	Название темы	Всего часов по дисциплине	Аудиторные часы		Самостоятельная работа
			Лекции	Семинары и практические занятия	
1	Основы компьютерной криминалистики	10	2	2	2
2	Эволюция целевых атак на банки и online fraud	10	2	2	2
3	Цифровая гигиена	10	2	2	4
4	Построение системы обеспечения ИБ в организации	10	2	2	4
5	Имитация атак. Взгляд изнутри	12	2	2	4
6	Реагирование на инциденты ИБ. Правовая база расследований киберпреступлений	12	4	4	8
7	Безопасность криптопроектов	12	2	2	6
8	OSINT – поиск информации по открытым источникам	18	4	4	6
<b>Итого по дисциплине</b>		76	20	20	36

## 6 Формы контроля знаний студентов

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
<b>Модуль 3</b>				T1				T2
<b>Модуль 4</b>				T3		ДЗ		ЭК

### 6.1 Порядок формирования оценок по дисциплине

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.*

## **7 Содержание дисциплины**

### **7.1 Содержание лекций**

#### **Лекция №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.

#### **Лекция №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

#### **Лекция №3.**

Цифровая гигиена

Краткое содержание:

- ◆ Безопасность электронной почты
- ◆ Безопасность паролей
- ◆ Безопасность мобильных 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

#### **Лекция №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

#### **Лекция №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

#### **Лекция №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

#### **Лекция №7**

## Безопасность криптопроектов

Краткое содержание:

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

## Лекция №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

## 8 Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Основная 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

### 8.2. 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

## **9 Материально-техническое обеспечение дисциплины**

- Проектор для проведения лекций и семинаров
- Классы для семинаров с компьютерами.