**Министерство науки и высшего образования РФ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Национальный исследовательский университет «МЭИ»**

---

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

# Рабочая программа дисциплины
# ОСНОВЫ ФОРЕНЗИКИ

| | |
|---|---|
| **Блок:** | **Блок 1 «Дисциплины (модули)»** |
| **Часть образовательной программы:** | **Часть, формируемая участниками образовательных отношений** |
| **№ дисциплины по учебному плану:** | **Б4.Ч.02** |
| **Трудоемкость в зачетных единицах:** | **3 семестр - 2;** |
| **Часов (всего) по учебному плану:** | **72 часа** |
| **Лекции** | **3 семестр - 16 часов;** |
| **Практические занятия** | **3 семестр - 16 часов;** |
| **Лабораторные работы** | **не предусмотрено учебным планом** |
| **Консультации** | **проводится в рамках часов аудиторных занятий** |
| **Самостоятельная работа** | **3 семестр - 39,7 часа;** |
| **в том числе на КП/КР** | **не предусмотрено учебным планом** |
| **Иная контактная работа** | **проводится в рамках часов аудиторных занятий** |
| **включая:**<br>**Семинар**<br>**Реферат**<br>**Контрольная работа** | |
| **Промежуточная аттестация:** | |
| **Зачет** | **3 семестр - 0,3 часа;** |

**Москва 2021**

**ПРОГРАММУ СОСТАВИЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность) | (подпись) | (расшифровка подписи) |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |
| Заведующий выпускающей кафедры | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** формирование знаний и практических навыков по основам форензики как науки, занимающейся отысканием свидетельств и доказательств при расследовании киберпреступлений и компьютерных инцидентов

**Задачи дисциплины**

- сформировать готовность и способность студентов к активному участию в процессе расследований компьютерных преступлений и инцидентов;;
- сформировать у студентов системный подход к методам и процессу сбора цифровых доказательств компьютерных преступлений и инцидентов и их закрепления;;
- выработать у студентов практические навыки правильного документального оформления результатов расследования компьютерных преступлений и инцидентов..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Запланированные результаты обучения** |
|---|---|---|
| ОПК-2 способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности | ИД-З$_{ОПК-2}$ Применяет программные средства прикладного назначения, в том числе отечественного производства для решения профессиональных задач | знать:<br>- технологию и этапы цифрового криминалистического процесса;;<br>- актуальность, перечень и механизм реализации типовых киберпреступлений;.<br><br>уметь:<br>- выполнять практические мероприятия по расследованию киберпреступлений и компьютерных инцидентов;;<br>- правильно фиксировать цифровые "следы" киберпреступлений и компьютерных инцидентов.. |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

| № п/п | Разделы/темы дисциплины/формы промежуточной аттестации | Всего часов на раздел | Семестр | Распределение трудоемкости раздела (в часах) по видам учебной работы | | | | | | | | | | Содержание самостоятельной работы/ методические указания |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Контактная работа | | | | | | | | СР | | |
| | | | | Лек | Лаб | Пр | Консультация | | ИКР | | ПА | Работа в семестре | Подготовка к аттестации /контроль | |
| | | | | | | | КПР | ГК | ИККП | ТК | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | Введение в форензику | 10.7 | 3 | 2 | - | 2 | - | - | - | - | - | 6.7 | - | ***Подготовка к аудиторным занятиям:*** Проработка материалов лекции, подготовка к практическому занятию ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Введение в форензику" ***Изучение материалов литературных источников:*** [3], 1-78 [4], 30-40 |
| 1.1 | Понятие, цель, методы, предмет, задачи и сфера применения форензики | 4.7 | | 1 | - | 1 | - | - | - | - | - | 2.7 | - | |
| 1.2 | Система обеспечения форензики | 6 | | 1 | - | 1 | - | - | - | - | - | 4 | - | |
| 2 | Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления. | 19 | | 5 | - | 2 | - | - | - | - | - | 12 | - | ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления." ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: - общая характеристика on-line мошенничества: |
| 2.1 | Общая характеристика типовых киберпреступлений | 10 | | 3 | - | 1 | - | - | - | - | - | 6 | - | |
| 2.2 | Общая характеристика криминалистического процесса и анализ его этапов. | 9 | | 2 | - | 1 | - | - | - | - | - | 6 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | способ, обстановка, преступник, потерпевший, следы; - общая характеристика экстремистских действий в сети: способ, обстановка, преступник, потерпевший, следы; - общая характеристика DoS и DDoS атаки: способ, обстановка, преступник, потерпевший, следы; - общая характеристика дефейса: способ, обстановка, преступник, потерпевший, следы; - общая характеристика распространения вредоносного кода: способ, обстановка, преступник, потерпевший, следы; - общая характеристика кардерства: способ, обстановка, преступник, потерпевший, следы; - общая характеристика мошенничества с трафиком: способ, обстановка, преступник, потерпевший, следы; - общая характеристика нарушения авторских прав в офлайне: способ, преступник, потерпевший, следы; - общая характеристика нарушения авторских прав в сети: способ, преступник, потерпевший, следы; - общая характеристика фишинга: способ, преступник, потерпевший; - общая характеристика кибersквоттинга; - общая характеристика терроризма и кибервойн: сценарии, методы реализации и противодействие.<br>***<u>Изучение материалов литературных источников:</u>***<br>[1], 1-72 |
| 3 | Организация оперативно-розыскных мероприятий методами форензики. | 42 | | 9 | - | 12 | - | - | - | - | - | 21 | - | ***<u>Подготовка домашнего задания:</u>***<br>Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Организация оперативно-розыскных мероприятий методами форензики." материалу. Дополнительно студенту необходимо изучить литературу и разобрать |
| 3.1 | Технология исследования трафика | 15 | | 3 | - | 4 | - | - | - | - | - | 8 | - | |
| 3.2 | Информативность, значение, технология | 15 | | 3 | - | 4 | - | - | - | - | - | 8 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | исследования содержания лог-файлов (логов) | | | | | | | | | | | | | примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. Тема домашнего задания: - организация перехвата и исследование трафика; - исследование статистики трафика с использованием специального программного обеспечения; - исследование лог-файлов Веб-сервера; - исследование системных логов Windows-систем; - исследование системных логов Linux-систем; - исследование лог-файлов мейл-сервера; - исследование принадлежности и расположения IP-адреса; - исследование принадлежности доменного имени; - исследование принадлежности адреса электронной почты; - исследование применения кейлоггеров. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Организация оперативно-розыскных мероприятий методами форензики." подготовка к выполнению заданий на практических занятиях ***Изучение материалов литературных источников:*** [2], 60-128 |
| 3.3 | Общая характеристика следственных действий методами форензики | 12 | | 3 | - | 4 | - | - | - | - | - | 5 | - | |
| | Зачет | 0.3 | | - | - | - | - | - | - | - | 0.3 | - | - | |
| | **Всего за семестр** | **72.0** | | **16** | **-** | **16** | **-** | **-** | **-** | **-** | **0.3** | **39.7** | **-** | |
| | **Итого за семестр** | **72.0** | | **16** | **-** | **16** | **-** | | **-** | | **0.3** | **39.7** | | |

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

**3.2 Краткое содержание разделов**

*1. Введение в форензику*

1.1. Понятие, цель, методы, предмет, задачи и сфера применения форензики
Изучение понятия, целей, методов, предмета, задач и сферы применения форензики.

1.2. Система обеспечения форензики
Изучение форензики с позиции системного подхода.

*2. Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления.*

2.1. Общая характеристика типовых киберпреступлений
On-line мошенничество, экстремистские действия в сети, DoS и DDoS атаки, "дефейс" интернет-сайтов, распространение вредоносного программного обеспечения, мошенничество с интернет-трафиком и др. Общая характеристика киберпреступлений и компьютерных инцидентов.

2.2. Общая характеристика криминалистического процесса и анализ его этапов.
Характеристика процессов сбора, исследования, анализа и представления результатов криминалистического процесса..

*3. Организация оперативно-розыскных мероприятий методами форензики.*

3.1. Технология исследования трафика
Значение, технология перехвата, статистическое исследование трафика.

3.2. Информативность, значение, технология исследования содержания лог-файлов (логов)
Содержание и информационная ценность системных, веб-, мейл, IP-адресов, доменных имен и др. логов.

3.3. Общая характеристика следственных действий методами форензики
Технология осмотра и изъятия компьютерной техники, работа с "короткоживущими и долгоживущими" данными, создание электронных "отпечатков", организация работы с потерпевшими,.

**3.3. Темы практических занятий**

1. Форензика: понятие, цели, методы, предмет, задачи, сфера применения. Семинар;
2. Компьютерные преступления: виды, способы совершения, "преступники", потерпевшие, характеристики следов. Семинар;
3. Организация оперативно-розыскных мероприятий: исследование трафика, исследование логов, исследование IP-адресов, исследование принадлежности, интернет-поиск. Круглый стол;
4. Компьютерно-техническая экспертиза: поиск и фиксация цифровых доказательств. Семинар;
5. Перехват и исследование трафика. Практическое занятие;
6. Исследование log-файлов. Практическое занятие;
7. Исследование IP-адресов компьютера, сервера. Практическое занятие.

**3.4. Темы лабораторных работ**

не предусмотрено

**3.5 Консультации**

*Групповые консультации по разделам дисциплины (ГК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Введение в форензику"

*Текущий контроль (ТК)*

1. Обсуждение материалов по кейсам раздела "Введение в форензику"
2. Консультации направлены на обеспечение правильного выполнения реферата (контрольного мероприятия) по разделу "Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления."
3. Консультации направлены на правильное выполнение домашнего задания по разделу "Организация оперативно-розыскных мероприятий методами форензики."

**3.6 Тематика курсовых проектов/курсовых работ**

Курсовой проект/ работа не предусмотрены

**3.7. Соответствие разделов дисциплины и формируемых в них компетенций**

| Запланированные результаты обучения по дисциплине (в соответствии с разделом 1) | Коды индикаторов | Номер раздела дисциплины (в соответствии с п.3.1) | | | Оценочное средство (тип и наименование) |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | |
| **Знать:** | | | | | |
| актуальность, перечень и механизм реализации типовых киберпреступлений; | ИД-З$_{ОПК-2}$ | | + | + | Реферат/Общая характеристика типовых киберпреступлений |
| технологию и этапы цифрового криминалистического процесса; | ИД-З$_{ОПК-2}$ | | + | | Контрольная работа/Организация оперативно-розыскных мероприятий методами форензики |
| **Уметь:** | | | | | |
| правильно фиксировать цифровые "следы" киберпреступлений и компьютерных инцидентов. | ИД-З$_{ОПК-2}$ | + | | + | Семинар/Изучение понятия, целей, методов, предмета, задач и сферы применения форензики |
| выполнять практические мероприятия по расследованию киберпреступлений и компьютерных инцидентов; | ИД-З$_{ОПК-2}$ | + | | + | Семинар/Изучение понятия, целей, методов, предмета, задач и сферы применения форензики |

## 4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

### 4.1. Текущий контроль успеваемости

**3 семестр**

Форма реализации: Выполнение задания

1. Общая характеристика типовых киберпреступлений (Реферат)

Форма реализации: Выступление (доклад)

1. Изучение понятия, целей, методов, предмета, задач и сферы применения форензики (Семинар)

Форма реализации: Письменная работа

1. Организация оперативно-розыскных мероприятий методами форензики (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

### 4.2 Промежуточная аттестация по дисциплине

*Зачет (Семестр №3)*

На основе оценок "зачет" по всем практическим заданиям и оценки "зачет" на зачете по дисциплине.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1 Печатные и электронные издания:

1. Capture the Flag [CTF]. Игровые модели подготовки специалистов в сфере компьютерной безопасности : [учебно-методическое пособие для преподавателей] / А. Ю. Егоров, А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИгеосистем, 2018 . – 72 с. - ISBN 978-5-8481-0232-1 .;
2. Анашкина, Н. В. Технологии и методы программирования : учебное пособие для вузов по направлению 090900 "Информационная безопасность", специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" / Н. В. Анашкина, Н. Н. Петухова, В. Ю. Смольянинов . – М. : Академия, 2012 . – 384 с. – (Высшее профессиональное образование . Бакалавриат) . - ISBN 978-5-7695-8429-9 .;
3. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
4. В. С. Пелешенко, С. В. Говорова, М. А. Лапина- "Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления", Издательство: "Северо-Кавказский Федеральный университет (СКФУ)", Ставрополь, 2017 -

(86 с.)
https://biblioclub.ru/index.php?page=book&id=467139.

**5.2 Лицензионное и свободно распространяемое программное обеспечение:**
1. СДО "Прометей";
2. Office;
3. Windows;
4. Майнд Видеоконференции;
5. Kali Linux;
6. ОС Linux;
7. Bootstrap.

**5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:**
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данных Scopus** - http://www.scopus.com
9. **Национальная электронная библиотека** - https://rusneb.ru/
10. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|---|---|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | М-511, Учебная аудитория | парта, стол преподавателя, стул, доска меловая |
| | К-601, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран |
| Учебные аудитории для проведения практических занятий, КР и КП | М-511, Учебная аудитория | парта, стол преподавателя, стул, доска меловая |
| | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| Учебные аудитории для проведения промежуточной аттестации | М-511, Учебная аудитория | парта, стол преподавателя, стул, доска меловая |
| | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| Помещения для самостоятельной работы | НТБ-303, Компьютерный читальный зал | стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер |
| | К-307, Учебная лаборатория "Открытое программное обеспечение" | стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в |

| | | |
|---|---|---|
| | | Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер |
| | К-302, Учебная лаборатория "Информационно-аналитические технологии" | стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер |
| Помещения для консультирования | М-511, Учебная аудитория | парта, стол преподавателя, стул, доска меловая |
| Помещения для хранения оборудования и учебного инвентаря | К-202/2, Склад кафедры БИТ | стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования |

**Приложение А**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Основы форензики

(название дисциплины)

**3 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Изучение понятия, целей, методов, предмета, задач и сферы применения форензики (Семинар)

КМ-2 Общая характеристика типовых киберпреступлений (Реферат)

КМ-3 Организация оперативно-розыскных мероприятий методами форензики (Контрольная работа)

**Вид промежуточной аттестации –** Зачет.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 |
|---|---|---|---|---|---|
| | | Неделя КМ: | 5 | 10 | 15 |
| 1 | Введение в форензику | | | | |
| 1.1 | Понятие, цель, методы, предмет, задачи и сфера применения форензики | | + | | |
| 1.2 | Система обеспечения форензики | | + | | |
| 2 | Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления. | | | | |
| 2.1 | Общая характеристика типовых киберпреступлений | | | + | |
| 2.2 | Общая характеристика криминалистического процесса и анализ его этапов. | | | | + |
| 3 | Организация оперативно-розыскных мероприятий методами форензики. | | | | |
| 3.1 | Технология исследования трафика | | + | | |
| 3.2 | Информативность, значение, технология исследования содержания лог-файлов (логов) | | | + | |
| 3.3 | Общая характеристика следственных действий методами форензики | | + | | |
| Вес КМ, %: | | | 30 | 30 | 40 |