**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**«Компьютерная криминалистика»**

Направление подготовки

**10.05.03 «Информационная безопасность автоматизированных систем»**

Образовательная программа (профиль)

**«Обеспечение информационной безопасности распределенных информационных систем»**

Квалификация (степень) выпускника

**Специалист**

Форма обучения

**Очная**

Год приема - 2019

Москва 2019 г.

## 1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Компьютерная криминалистика» следует отнести:

- 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.

К **основным задачам** освоения дисциплины «Компьютерная криминалистика» следует отнести:

- знание основ компьютерной криминалистики, правовых норм расследований инцидентов информационной безопасности, алгоритмов расследований инцидентов информационной безопасности;
- умение самостоятельно проводить расследования инцидентов информационной безопасности, проводить компьютерно-техническую экспертизу;
- приобретение опыта поиска цифровых следов в компьютерных системах, фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, документирования противоправных действий злоумышленника.

## 2. Место дисциплины в структуре ООП.

Дисциплина «Компьютерная криминалистика» относится к числу профессиональных учебных дисциплин по выбору студента части цикла (Б.1.ДВ) основной образовательной программы (Б.1.ДВ.4).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Организационное и правовое обеспечение информационной безопасности, Безопасность сетей электронных вычислительных машин, Безопасность операционных систем, Защита конфиденциальной информации и персональных данных.

## 3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

| **Код компетенции** | **В результате освоения образовательной программы** | **Перечень планируемых результатов обучения по дисциплине** |
|---|---|---|

| | **обучающийся должен обладать** | |
|---|---|---|
| ПК-17 | Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | **Знать:**<br>• основы компьютерной криминалистики;<br>• правовые нормы расследований инцидентов информационной безопасности;<br>• алгоритмы расследований инцидентов информационной безопасности;<br>**Уметь:**<br>• самостоятельно проводить расследования инцидентов информационной безопасности;<br>• проводить компьютерно-техническую экспертизу;<br>• документировать противоправные действия злоумышленника.<br>**Владеть:**<br>• методами поиска цифровых следов в компьютерных системах;<br>• методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>• навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы. |

## 4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 6 семестре.

Структура и содержание дисциплины «Компьютерная криминалистика» по срокам и видам работы отражены в приложении.

### Содержание разделов дисциплины

### Тема 1. Основы компьютерной криминалистики.

Введение в компьютерную криминалистику. Особенности современных подходов: Windows криминалистика, криминалистика оперативной памяти, криминалистика мобильных устройств, криминалистика сетевого траффика.

**Тема 2. Эволюция целевых атак на банки и online fraud.**

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.

**Тема 3. Цифровая гигиена**.

Безопасность электронной почты. Безопасность паролей. Безопасность мобильных приложений. Безопасность компьютеров. Безопасность браузеров. Безопасность соц. Сетей.

**Тема 4. Реагирование на инциденты ИБ. Правовая база расследований киберпреступлений.**

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

**Тема 5. Поиск информации по открытым источникам.**

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

## 5. Образовательные технологии.

Методика преподавания дисциплины «Компьютерная криминалистика» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

Образцы тестовых заданий, экзаменационных билетов, приведены в приложении.

### 6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

| Код компетенции | В результате освоения образовательной программы обучающийся должен обладать |
|---|---|
| ПК-17 | Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации |

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

### 6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

| ПК-17 Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| **знать:**<br>•основы компьютерной криминалистики;<br>•правовые нормы расследований инцидентов информационной безопасности;<br>•алгоритмы расследований инцидентов информационной безопасности. | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний:<br>•основы компьютерной криминалистики;<br>•правовые нормы расследований инцидентов информационной безопасности;<br>•алгоритмы расследований инцидентов информационной безопасности.. | Обучающийся демонстрирует неполное соответствие следующих знаний:<br>•основы компьютерной криминалистики;<br>•правовые нормы расследований инцидентов информационной безопасности;<br>•алгоритмы расследований инцидентов информационной безопасности.<br>Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при | Обучающийся демонстрирует частичное соответствие следующих знаний:<br>•основы компьютерной криминалистики;<br>•правовые нормы расследований инцидентов информационной безопасности;<br>•алгоритмы расследований инцидентов информационной безопасности, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует полное соответствие следующих знаний:<br>•основы компьютерной криминалистики;<br>•правовые нормы расследований инцидентов информационной безопасности;<br>•алгоритмы расследований инцидентов информационной безопасности, свободно оперирует приобретенными знаниями. |

| | | | | |
|---|---|---|---|---|
| | | оперировании знаниями при их переносе на новые ситуации. | | |
| **уметь:**<br>•самостоятельно проводить расследования инцидентов информационной безопасности;<br>•проводить компьютерно-техническую экспертизу;<br>•документировать противоправные действия злоумышленника. | Обучающийся не умеет или в недостаточной степени умеет<br>•самостоятельно проводить расследования инцидентов информационной безопасности;<br>•проводить компьютерно-техническую экспертизу;<br>•документировать противоправные действия злоумышленника. | Обучающийся демонстрирует неполное соответствие следующих умений:<br>•самостоятельно проводить расследования инцидентов информационной безопасности;<br>•проводить компьютерно-техническую экспертизу;<br>•документировать противоправные действия злоумышленника.<br>Допускаются значительные ошибки, проявляется недостаточность умений. | Обучающийся демонстрирует частичное соответствие следующих умений:<br>•самостоятельно проводить расследования инцидентов информационной безопасности;<br>•проводить компьютерно-техническую экспертизу;<br>•документировать противоправные действия злоумышленника.<br>Умения освоены, но допускаются незначительные ошибки, неточности. | Обучающийся демонстрирует полное соответствие следующих умений:<br>•самостоятельно проводить расследования инцидентов информационной безопасности;<br>•проводить компьютерно-техническую экспертизу;<br>•документировать противоправные действия злоумышленника.<br>Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:**<br>•методами поиска цифровых следов в компьютерных системах;<br>•методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>•навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы. | Обучающийся не владеет или в недостаточной степени владеет<br>•методами поиска цифровых следов в компьютерных системах;<br>•методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>•навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы. | Обучающийся владеет<br>•методами поиска цифровых следов в компьютерных системах;<br>•методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>•навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, но допускаются значительные ошибки, проявляется недостаточность владения | Обучающийся частично владеет<br>•методами поиска цифровых следов в компьютерных системах;<br>•методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>•навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, навыки освоены, но допускаются незначительные | Обучающийся в полном объеме владеет<br>•методами поиска цифровых следов в компьютерных системах;<br>•методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>•навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы, свободно применяет полученные навыки |

| | | | | |
|---|---|---|---|---|
| | | | ошибки, неточности, затруднения. | в ситуациях повышенной сложности. |

Шкалы оценивания результатов промежуточной аттестации и их описание:

***Форма промежуточной аттестации: экзамен.***

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| **Шкала оценивания** | **Описание** |
|---|---|
| Отлично | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. |
| Удовлетворительно | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. |
| Неудовлетворительно | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

**Фонды оценочных средствпредставлены в приложении к рабочей программе.**

## 7. Учебно-методическое и информационное обеспечение дисциплины.

**а) основная литература:**


1. Федотов Николай Николаевич. Форензика - компьютерная криминалистика [Текст] / Николай Николаевич Федотов. - 2-е изд. - Москва : OneBook.ru, 2012. - 418, [1] с. : ил., табл.; 25 см.; ISBN 978-5-905948-22-0


**б) дополнительная литература:**


2. Michael K Robinson. Digital Forensics Workbook: Hands-on Activities in Digital Forensics
3. John Sammons. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics
4. Cory Altheide, Harlan Carvey. Digital Forensics with Open Source Tools.
5. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for our Connected World
6. Brian Krebs. Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door
7. Kevin Mitnick. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker
8. C. Warren Axelrod. Enterprise Information Security and Privacy
9. Gerardus Blokdyk. Enterprise Information Security Architecture: The Ultimate Step-By-Step Guide 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
14. Peter Kim. The Hacker Playbook: Practical Guide To Penetration Testing
15. Chris Sanders. Applied Network Security Monitoring: Collection, Detection, and Analysis
16. Michael Collins. Network Security Through Data Analysis: Building Situational Awareness


## 8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

## 9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

## 10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем».**

**Программу составил:** к.т.н., доцент Н.В. Федоров

**Программа утверждена на заседании кафедры “Информационная безопасность”** «29» августа 2019 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

**Структура и содержание дисциплины «Компьютерная криминалистика»**
**по направлению подготовки**
**10.05.03 «Информационная безопасность автоматизированных систем»**
**(специалист)**

| n/n | Раздел | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах | | | | | Виды самостоятельной работы студентов | | | | | Формы аттестации | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Л | П/С | Лаб | СРС | КСР | К.Р. | К.П. | ДЗ | Реферат | К/р | Э | З |
| | **6 семестр** | | | | | | | | | | | | | | |
| 1 | Тема 1. Основы компьютерной криминалистики. | 6 6 | 1-2 | | | 8 | 8 | | | | | | | | |
| 2 | Тема 2. Эволюция целевых атак на банки и online fraud. | | 3-4 | | | 8 | 8 | | | | | | | | |
| 3 | Тема 3. Цифровая гигиена. | | 5-8 | | | 16 | 16 | | | | | | | | |
| 4 | Тема 4. Реагирование на инциденты ИБ. Правовая база расследований киберпреступлений. | | 9-13 | | | 20 | 20 | | | | | | | | |
| 5 | Тема 5. Поиск информации по открытым источникам. | | 14-18 | | | 20 | 20 | | | | | | | | |
| | ***Форма аттестации*** | | 19-21 | | | | | | | . | | | | Э | |
| | Всего часов по дисциплине во шестом семестре | | | | | 72 | 72 | | | | | | | | |
| | **Всего часов по дисциплине** | | | | | 72 | 72 | | | | | | | | |

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ПО ДИСЦИПЛИНЕ

## «Компьютерная криминалистика»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

**Составители: доц. Федоров Н.В.**

Москва, 2019 год

Таблица 1

**ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

| **Компьютерная криминалистика** | | | | | |
|---|---|---|---|---|---|
| ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»** | | | | | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**: | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технология формирования компетен** | **Форма оценоч-ного** | **Степени уровней освоения компетенций** |
| **ИН-ДЕКС** | **ФОРМУЛИРОВКА** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| ПК-17 | Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | **Знать:**<br>• основы компьютерной криминалистики;<br>• правовые нормы расследований инцидентов информационной безопасности;<br>• алгоритмы расследований инцидентов информационной безопасности;<br>**Уметь:**<br>• самостоятельно проводить расследования инцидентов информационной безопасности;<br>• проводить компьютерно-техническую экспертизу;<br>• документировать противоправные действия злоумышленника.<br>**Владеть:**<br>• методами поиска цифровых следов в компьютерных системах;<br>• методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>• навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы. | самостоятельная работа, лабораторные занятия | экзамен | **Базовый уровень:**<br>**Знать:**<br>• основы компьютерной криминалистики;<br>• правовые нормы расследований инцидентов информационной безопасности;<br>• алгоритмы расследований инцидентов информационной безопасности;<br>**Уметь:**<br>• проводить компьютерно-техническую экспертизу;<br>• документировать противоправные действия злоумышленника.<br>**Владеть:**<br>• методами поиска цифровых следов в компьютерных системах;<br>• методами фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;<br>Повышенный уровень:<br>**Уметь:**<br>• самостоятельно проводить расследования инцидентов информационной безопасности;<br>**Владеть:**<br>• навыками анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы. |

Приложение 2
к рабочей программе

**Оценочные средства для промежуточной аттестации**

**Экзамен.**

**Список вопросов для экзамена по дисциплине**

1. Основные направления деятельности группировки Lazarus
2. Основные направления деятельности группировки Silence
3. Основные направления деятельности группировки Cobalt
4. o\Основные направления деятельности группировки Moneytaker
5. Darkshops, Malware, Botnets
6. Отмывание денег, Спам, Фишинг, Cybercrime to Cybercrime
7. Threat Intelligence. Существующие платформы.
8. STIX, TAXII Protocols
9. Honeypots. Зачем нужны и как использовать
10. Стратегическая кибербразведка
11. Операционная кибербразведка
12. Тактическая кибербразведка
13. OSINT
14. Tor. Как работает
15. Подходы к деанонимизации TOR
16. Что такое «блокчейн» и «криптовалюты»?
17. Основные киберугрозы для участников криптоиндустрии. ICO
18. Основные киберугрозы для участников криптоиндустрии. Смарт-контракты
19. Основные киберугрозы для участников криптоиндустрии. Криптобиржи
20. Основные киберугрозы для участников криптоиндустрии. Криптофонды
21. Основные киберугрозы для участников криптоиндустрии. Майнеры
22. Крупные и успешные кибератаки на проекты блокчейн индустрии
23. Защита интеллектуальной собственности в интернете

Пример билета.

1. Стратегическая кибербразведка
2. Основные киберугрозы для участников криптоиндустрии. Смарт-контракты