

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Максимов Алексей Борисович

Должность: директор департамента по образовательной политике

Дата подписания: 05.09.2026 14:03:59

Уникальный программный ключ:

8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

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

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета

«Информационных технологий»



/ Д.Г. Демидов /

« 26 » февраля 2026 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы форензики»

Направление подготовки

**10.03.01 «Информационная безопасность»**

Профиль/специализация

**«Безопасность компьютерных систем»**

Квалификация

**Бакалавр**

Формы обучения

**Очная**

Москва, 2026 г.

**Разработчик(и):**

Преподаватель



/Г.Ф. Шипулин/

**Согласовано:**

Заведующий кафедрой «Информационная безопасность»



/И.В.Калуцкий/

Руководитель образовательной программы,



А.Ю. Гневшев

## Содержание

|     |                                                                              |   |
|-----|------------------------------------------------------------------------------|---|
| 1   | Цели, задачи и планируемые результаты обучения по дисциплине                 | 4 |
| 2   | Место дисциплины в структуре образовательной программы                       | 4 |
| 3   | Структура и содержание дисциплины                                            | 4 |
| 3.1 | Виды учебной работы и трудоемкость                                           | 4 |
| 3.2 | Тематический план изучения дисциплины                                        | 6 |
| 3.3 | Содержание дисциплины                                                        | 7 |
| 3.4 | Тематика семинарских/практических и лабораторных занятий                     | 7 |
| 3.5 | Тематика курсовых проектов (курсовых работ)                                  | 7 |
| 4   | Учебно-методическое и информационное обеспечение                             | 7 |
| 4.1 | Нормативные документы и ГОСТы                                                | 7 |
| 4.2 | Основная литература                                                          | 7 |
| 4.3 | Дополнительная литература                                                    | 7 |
| 4.4 | Электронные образовательные ресурсы                                          | 8 |
| 4.5 | Лицензионное и свободно распространяемое программное обеспечение             | 8 |
| 4.6 | Современные профессиональные базы данных и информационные справочные системы | 8 |
| 5   | Материально-техническое обеспечение                                          | 8 |
| 6   | Методические рекомендации                                                    | 8 |
| 6.1 | Методические рекомендации для преподавателя по организации обучения          | 8 |
| 6.2 | Методические указания для обучающихся по освоению дисциплины                 | 8 |
| 7   | Фонд оценочных средств                                                       | 9 |
| 7.1 | Методы контроля и оценивания результатов обучения                            | 9 |
| 7.2 | Шкала и критерии оценивания результатов обучения                             | 9 |
| 7.3 | Оценочные средства                                                           | 9 |

## 1 Цели, задачи и планируемые результаты обучения по дисциплине

**Целью** преподавания дисциплины является формирование у студентов знаний в области форензики, сбора и анализа цифровых доказательств.

**Задачи** преподавания дисциплины:

- изучение этапов, методов и средств проведения компьютерно-технических экспертиз;
- освоение способов и методов средств сбора цифровых доказательств;
- освоение методов организации и управления деятельности служб защиты информации на предприятии.

В результате освоения дисциплины «Основы форензики» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

знать:

- принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);

уметь:

- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;

владеть:

- методами организации и управления деятельность служб защиты информации на предприятии.

Обучение по дисциплине «Основы форензики» направлено на формирование у обучающихся следующих компетенций:

| Код и наименование компетенций                                                                                                                                                         | Индикаторы достижения компетенции                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; | ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);<br>ИПК-6.2. Владеет методами организации и управления деятельность служб защиты информации на предприятии. |

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Основы форензики» относится к числу элективных профессиональных учебных дисциплин части, формируемой участниками образовательных отношений (Б1.ЭД) основной образовательной программы (Б1.ЭД.3).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Мониторинг событий и управление инцидентами (SIEM)», «Основы управления информационной безопасностью».

## 3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, т.е. 144 часов (лекции – 4 часов, лабораторные занятия – 68 часа, самостоятельная работа - 72 часа, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Основы форензики» по срокам и видам работы отражены в приложении

### 3.1 Виды учебной работы и трудоемкость

(по формам обучения)

#### 3.1.1 Очная форма обучения

| №<br>п/п | Вид учебной работы               | Количество<br>часов | Семестры |  |
|----------|----------------------------------|---------------------|----------|--|
|          |                                  |                     | 7        |  |
| <b>1</b> | <b>Аудиторные занятия</b>        | <b>72</b>           | 72       |  |
|          | В том числе:                     |                     |          |  |
| 1.1      | Лекции                           | 4                   | 4        |  |
| 1.2      | Семинарские/практические занятия |                     |          |  |
| 1.3      | Лабораторные занятия             | 68                  | 68       |  |
| <b>2</b> | <b>Самостоятельная работа</b>    | <b>72</b>           | 72       |  |
|          | В том числе:                     |                     |          |  |
| 2.1      | ...                              |                     |          |  |
| <b>3</b> | <b>Промежуточная аттестация</b>  |                     |          |  |
|          | Зачет/диф.зачет/экзамен          |                     | Экзамен  |  |
|          | <b>Итого</b>                     | <b>144</b>          |          |  |

#### 3.1.2 Очно-заочная форма обучения

Не предусмотрена

#### 3.1.3 Заочная форма обучения

Не предусмотрена

### 3.2 Тематический план изучения дисциплины

(по формам обучения)

#### 3.2.1 Очная форма обучения

| №<br>п/п | Разделы/темы<br>дисциплины      | Трудоемкость, час |                   |                                                 |                                     |                                        |                                           |
|----------|---------------------------------|-------------------|-------------------|-------------------------------------------------|-------------------------------------|----------------------------------------|-------------------------------------------|
|          |                                 | Всего             | Аудиторная работа |                                                 |                                     |                                        | Само<br>стоят<br>ельна<br>я<br>работ<br>а |
|          |                                 |                   | Лекц<br>ии        | Семина<br>рские/<br>практич<br>еские<br>занятия | Лабор<br>аторн<br>ые<br>заняти<br>я | Практ<br>ическа<br>я<br>подго<br>товка |                                           |
| 1        | Раздел 1.                       |                   |                   |                                                 |                                     |                                        |                                           |
| 1.1      | Тема 1. Введение в форензику.   | 8                 | 4                 |                                                 |                                     |                                        | 4                                         |
| 1.2      | Тема 2. Компьютерная форензика. | 72                |                   |                                                 | 36                                  |                                        | 36                                        |
| 1.3      | Тема 3. Сетевая форензика.      | 64                |                   |                                                 | 32                                  |                                        | 32                                        |
|          | <b>Итого</b>                    | <b>144</b>        | <b>4</b>          |                                                 | <b>68</b>                           |                                        | <b>72</b>                                 |

#### 3.2.2 Очно-заочная форма обучения

Не предусмотрена.

3.2.2 Заочная форма обучения  
Не предусмотрена

### 3.3. Содержание дисциплины

| № п/п | Раздел (тема) дисциплины | Содержание                                                                                                                                                                                                                                                                                                                                                    |
|-------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | 2                        | 3                                                                                                                                                                                                                                                                                                                                                             |
| 1     | Раздел 1                 |                                                                                                                                                                                                                                                                                                                                                               |
| 1.1   | Введение в форензику.    | Форензика: определение, классификация, цели и задачи, разбор практических кейсов. Компьютерная экспертиза: определение, классификация, этапы проведения. СОРМ.                                                                                                                                                                                                |
| 1.2   | Компьютерная форензика.  | Устройство hdd, ssd и flash накопителей. Способы и средства анализа файловых систем, восстановление данных, метаданные файлов. Программные и аппаратные средства копирования носителей информации. RAM-память: устройство, инструментальные средства копирования и анализа. Анализ систем под управлением ОС Windows. Анализ систем под управлением ОС Linux. |
| 1.3   | Сетевая форензика.       | Межсетевые экраны, IPS, IDS, SIEM-решения. Аудит событий ОС Linux, Windows. Методы и способы выявления сетевых атак на основе анализа трафика.                                                                                                                                                                                                                |

### 3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

*Не предусмотрены учебным планом.*

3.4.2 Лабораторные занятия

| №     | Наименование лабораторной работы            | Объем, час. |
|-------|---------------------------------------------|-------------|
| 1     | Выполнение лабораторной работы №1 по теме 2 | 36          |
| 2     | Выполнение лабораторной работы №2 по теме 3 | 32          |
| Итого |                                             | 68          |

### 3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

## 4 Учебно-методическое и информационное обеспечение

### 4.4 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность».

#### 4.5 Основная литература

1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167606> (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 8.
2. Кеворкова, Ж.А. МЕТОДИЧЕСКИЕ АСПЕКТЫ ФОРЕНЗИК-КОНТРОЛЯ КАК ИНСТРУМЕНТА ВЫЯВЛЕНИЯ И ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В ДЕЯТЕЛЬНОСТИ ЭКОНОМИЧЕСКИХ СУБЪЕКТОВ / Ж. А. Кеворкова // Вестник Воронежского государственного университета. Серия: Экономика и управление. — 2020. — № 4. — С. 43-53. — ISSN 1814-2966. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/journal/issue/316342> (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1.
3. Федотов Н.Н. Форензика – компьютерная криминалистика –М.: Юридический Мир, 2007. — 432

#### 4.6 Дополнительная литература

1. Криминалистика : учебное пособие / В. В. Яровенко, Н. М. Букаев, Г. С. Воропаев [и др.] ; под редакцией В. В. Яровенко. — Владивосток : ВГУЭС, 2020. — ISBN 978-5-9736-0617-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/250313> (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 42.
2. Информационная безопасность: современная теория и практика: сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции : сборник научных трудов / под редакцией З. В. Семеновой. — Омск : СиБАДИ, 2019. — ISBN 978-5-00113-134-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163756> (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 87.

#### 4.7 Электронные образовательные ресурсы

1. ЭОР «Основы форензики» [Электронный ресурс] — URL: <https://online.mospolytech.ru/course/view.php?id=10983> (дата обращения: 18.02.2023).

#### 4.8 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Дистрибутив ОС Kali Linux
4. Дистрибутив ОС Windows Server 2012/2016
5. Дистрибутив ОС Windows 7, 10

## **4.9 Современные профессиональные базы данных и информационные справочные системы**

1. Сайт Федеральной службы безопасности России (ФСБ России). -<http://www.fsb.ru>.
2. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). -  
<http://www.fstec.ru>.
3. Портал технического комитета по стандартизации «Защита информации». –  
<http://tk.gost.ru/wps/portal/tk362>

## **5 Материально-техническое обеспечение**

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.

## **6 Методические рекомендации**

### **6.4 Методические рекомендации для преподавателя по организации обучения**

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

### **6.5 Методические указания для обучающихся по освоению дисциплины**

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

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.

## **7 Фонд оценочных средств**

### **7.4 Методы контроля и оценивания результатов обучения**

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

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;

- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

## 7.5 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

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.                           |

## 7.6 Оценочные средства

### 7.3.1 Текущий контроль

Оценочные средства для текущей аттестации

- Защита отчетов о выполнении лабораторных работ

### 7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

- Экзамен

Список вопросов для проведения экзамена по дисциплине:

1. Формензика: определение, классификация, цели и задачи.
2. Компьютерная экспертиза: определение, классификация, используемое ПО.
3. Виды и архитектура СОРМ.
4. Устройство hdd, ssd и flash накопителей.
5. Способы и средства анализа файловых систем.
6. Программные и аппаратные средства копирования носителей информации.
7. RAM-память: устройство, инструментальные средства копирования и анализа.
8. Анализ систем под управлением ОС Windows.
9. Анализ систем под управлением ОС Linux.
10. Межсетевые экраны.
11. Системы обнаружения и предотвращения вторжений.
12. SIEM-системы.
13. Аудит событий ОС Linux.
14. Аудит событий ОС Windows.
15. Методы и способы выявления сетевых атак на основе анализа трафика.
16. Способы и средства восстановления данных.
17. Способы и средства извлечения и анализа метаданных файлов.
18. Этапы проведения компьютерных экспертиз.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ

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

---

Факультет информационных технологий  
Кафедра: Информационная безопасность  
Дисциплина: Основы форензики  
Бакалавры. Курс 4, семестр 1

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Аудит событий ОС Linux.
2. Этапы проведения компьютерных экспертиз.

Преподаватель \_\_\_\_\_ / Шипулин Г.Ф. /

---