

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
"Дальневосточный государственный университет путей сообщения"  
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и  
системы

Попов М.А., канд. техн.  
наук, доцент



11.06.2021

## РАБОЧАЯ ПРОГРАММА

дисциплины **Форензика**

для направления подготовки 09.04.02 Информационные системы и технологии

Составитель(и): к.т.н., Доцент, Попов М.А.

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 09.06.2021г. № 6

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от  
11.06.2021 г. № 6

г. Хабаровск  
2022 г.

---

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2023 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2024 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2025 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2026 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины **Форензика**

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 917

Квалификация **магистр**

Форма обучения **очная**

**ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		экзамены (семестр) 4
контактная работа	38	РГР 4 сем. (1)
самостоятельная работа	70	
часов на контроль	36	

**Распределение часов дисциплины по семестрам (курсам)**

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		Итого	
	7 1/6			
Неделя				
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	6	6	6	6
В том числе инт.	8	8	8	8
Итого ауд.	32	32	32	32
Контактная работа	38	38	38	38
Сам. работа	70	70	70	70
Часы на контроль	36	36	36	36
Итого	144	144	144	144

### 1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Введение. Предмет. Форензика и прогресс. Задачи. Общенаучные методы. Специальные методы. Роль экспертно-криминалистических подразделений. Современное состояние. Специальные технические средства: Аппаратные средства. Экспертные программы. Наборы хэшей. Архивирование. Значение спецсредств. Криминалистические информационные системы. Компьютерные преступления. Криминалистическая характеристика. Статистика. Личность вероятного преступника. Оперативность. Приоритетность расследования. Онлайн-мошенничество: Клевета, оскорбления и экстремистские действия в Сети. DoS-атаки. Дефейс. Вредоносные программы. Кардерство. Мошенничество с трафиком. Нарушение авторских прав. Оперативно-розыскные мероприятия. Перехват и исследование трафика. Шифрованный трафик. Анализ заголовков пакетов. Другие данные о трафике. Установление принадлежности и расположения IP-адреса. Установление принадлежности доменного имени. Принадлежность адреса электронной почты. Следственные действия. Компьютерно-техническая экспертиза. Перспективы.
-----	---

### 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код дисциплины:	Б1.В.ДВ.03.02
<b>2.1</b>	<b>Требования к предварительной подготовке обучающегося:</b>
2.1.1	Компьютерные, сетевые и информационные технологии
2.1.2	Планирование научного эксперимента и обработка экспериментальных данных
<b>2.2</b>	<b>Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>
2.2.1	Научно-исследовательская работа

### 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

**ПК-3: Способен проводить разработку и исследование методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий**

**Знать:**

Теоретические основы разработки и исследования методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий в области безопасности баз данных; современных серверов баз данных; корпоративных систем; защите конфиденциальных документов; информационных процессах; программирования; информационных WEB-систем.

**Уметь:**

Использовать разработки и исследования методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий в области безопасности баз данных; современных серверов баз данных; корпоративных систем; защите конфиденциальных документов; информационных процессах; программирования; информационных WEB-систем.

**Владеть:**

Навыками разработки и исследования методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий в области безопасности баз данных; современных серверов баз данных; корпоративных систем; защите конфиденциальных документов; информационных процессах; программирования; информационных WEB-систем.

#### ПК-7: Способен прогнозировать развитие информационных систем и технологий

**Знать:**

Современные информационные системы и технологии в криптографии; кодировании и передачи информации и прогнозировать их развитие.

**Уметь:**

Применять современные информационные системы и технологии в криптографии; кодировании и передачи информации и прогнозировать их развитие.

**Владеть:**

Навыками применения современных информационных систем и технологий в криптографии; кодировании и передачи информации и прогнозирования их развития.

### 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						

1.1	Введение. Предмет. Форензика и прогресс. Задачи. Общенаучные методы. Специальные методы. Роль экспертно-криминалистических подразделений. Современное состояние. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.2	Специальные технические средства: Аппаратные средства. Экспертные программы. Наборы хэшей. Архивирование. Значение спецсредств. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.3	Криминалистические информационные системы. Компьютерные преступления. Криминалистическая характеристика. Статистика. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.4	Личность вероятного преступника. Оперативность. Приоритетность расследования. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.5	Онлайн-мошенничество: Клевета, оскорбления и экстремистские действия в Сети. DoS-атаки. Дефейс. Вредоносные программы. Кардерство Мошенничество с трафиком. Нарушение авторских прав. Оперативно -розыскные мероприятия. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.6	Перехват и исследование трафика. Шифрованный трафик. Анализ заголовков пакетов. Другие данные о трафике. Установление принадлежности и расположения IP-адреса. Установление принадлежности доменного имени. Принадлежность адреса электронной почты. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.7	Следственные действия. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.8	Компьютерно-техническая экспертиза. Перспективы. /Лек/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
<b>Раздел 2. Лабораторные</b>							
2.1	Перехват и исследование трафика /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.2	Исследование логов веб-сервера /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.3	Исследование системных логов /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.4	Исследование логов мейл-сервера и заголовков электронной почты /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.5	Установление принадлежности и расположения IP-адреса /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.6	Установление принадлежности доменного имени /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.7	Принадлежность адреса электронной почты /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.8	Кейлогеры /Пр/	4	2	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	

	<b>Раздел 3. Самостоятельная работа</b>						
3.1	Подготовка к лекциям /Ср/	4	8	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.2	Подготовка к практическим работам /Ср/	4	30	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.3	Расчетно-графические работы /Ср/	4	32	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.4	/Экзамен/	4	36	ПК-3 ПК-7	Л1.1Л2.1 Л2.2 Э1 Э2	0	

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1. Рекомендуемая литература

#### 6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Русскевич Е. А.	Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2017, <a href="http://znanium.com/go.php?id=776078">http://znanium.com/go.php?id=776078</a>

#### 6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Айков Д., Сейгер К.	Компьютерные преступления.Руководство по борьбе с компьютерными преступлениями	Москва: Мир, 1999,
Л2.2	Борисов С.	Преступления в сфере компьютерной информации	Москва: Лаборатория книги, 2010, <a href="http://biblioclub.ru/index.php?page=book&amp;id=101046">http://biblioclub.ru/index.php?page=book&amp;id=101046</a>

#### 6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	Н.Н.Федотов Форензика – компьютерная криминалистика	<a href="https://forensics.ru/">https://forensics.ru/</a>
Э2	Компьютерная криминалистика (форензика) — обзор инструментария и тренировочных площадок	<a href="https://habr.com/ru/post/327740/">https://habr.com/ru/post/327740/</a>

#### 6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

##### 6.3.1 Перечень программного обеспечения

Microsoft Windows XP SP3

Microsoft Office Professional 2007

Free Conference Call (свободная лицензия)

Zoom (свободная лицензия)

##### 6.3.2 Перечень информационных справочных систем

## 7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки

Аудитория	Назначение	Оснащение
		Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742,
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая

### 8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Занятия по дисциплине «Форензика» реализуются с использованием как активных, так и интерактивных форм обучения, позволяющих взаимодействовать в процессе обучения не только преподавателю и студенту, но и студентам между собой.

В соответствии с учебным планом для слушателей дневного отделения изучение курса предполагает выполнение установленного комплекса практических работ (в аудитории), а также расчетно-графических работ (самостоятельно) в течение одного семестра.

Необходимый и достаточный для успешного выполнения практической работы объем теоретического материала изложен в методических указаниях или выдается преподавателем на занятиях. При выполнении задания должны соблюдаться все требования или условия, обозначенные в условиях практических заданий.

Практическая работа считается выполненной, если студент смог продемонстрировать на лабораторном стенде – ПК с соответствующим программным обеспечением правильный результат и пояснить ход выполнения работы.

При выполнении РГР студент должен руководствоваться лекционным материалом, а также обязательно использовать другие литературные источники по своему усмотрению, в частности, приведенные в РПД дисциплины. В ходе выполнения каждой РГР студент на изучаемых ранее языках и технологиях программирования должен создать несколько вариантов тематического (в соответствии с заданным вариантом) приложения, реализующего предусмотренные заданием функционал. После завершения выполнения каждой РГР слушатель допускается к защите и демонстрации приложения. Защита РГР проходит в форме собеседования по вопросам, касающихся причин применения и особенностей реализации предложенных программных решений.

Текущий контроль знаний студентов осуществляется на практических занятиях в соответствии с тематикой работ путем устного опроса, а также при защите РГР. Кроме этого в середине семестра проводится промежуточная аттестация студентов дневной формы обучения, согласно рейтинговой системе ДВГУПС.

Студент, своевременно выполнивший все предусмотренные программой практические работы и защитивший РГР допускается к зачету. Выходной контроль знаний слушателей осуществляется на зачете в конце семестра в форме собеседования или тестирования.

Темы РГР.

#### 1. Перехват и исследование трафика

Вопросы

1. Исследование логов веб-сервера
2. Исследование системных логов
3. Исследование логов мейл-сервера и заголовков электронной почты

#### 2. Установление принадлежности источника

Вопросы:

1. Установление принадлежности и расположения IP-адреса
2. Установление принадлежности доменного имени
3. Принадлежность адреса электронной почты

#### 4. Кейлогеры

Отчет должен соответствовать следующим требованиям:

1. Отчет результатов РГР оформляется в текстовом редакторе MS Word на листах формата А4 (297x210).
2. Изложение материала в отчете должно быть последовательным и логичным. Отчет состоит из задания на РГР, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем РГР работы должен быть – 10-15 страниц.
4. Отчет должен быть отпечатан на компьютере через 1-1,5 интервала, номер шрифта – 12-14 пт Times New Roman. Расположение текста должно обеспечивать соблюдение следующих полей:
  - левое 20 мм.
  - правое 15 мм.
  - верхнее 20 мм.
  - нижнее 25 мм.
5. Все страницы отчета, включая иллюстрации и приложения, имеют сквозную нумерацию без пропусков, повторений, литературных добавлений. Первой страницей считается титульный лист, на которой номер страницы не ставится.
6. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
7. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
8. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.
9. Ссылки на литературный источник в тексте сопровождаются порядковым номером, под которым этот источник включен в список используемой литературы. Перекрестная ссылка заключается в квадратные скобки. Допускаются постраничные сноски с фиксированием источника в нижнем поле листа.
10. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

Оформление и защита производится в соответствии со стандартом ДВГУПС СТ 02-11-17 «Учебные студенческие работы. Общие положения»

Оценка знаний по дисциплине производится в соответствии со стандартом ДВГУПС СТ 02-28-14 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации»