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**

10.04.01 Информационная безопасность

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 26.11.2020 № 1455

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
контактная работа 58
самостоятельная работа 50

Виды контроля в семестрах:
зачёты с оценкой 4
РГР 4 сем. (1)

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семест р на курсе>)	**4 (2.2)**		Итого	
Недель	6 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	32	32	32	32
Контроль самостоятельной работы	10	10	10	10
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	58	58	58	58
Сам. работа	50	50	50	50
Итого	108	108	108	108

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. Экс-пертные программы. Наборы хэшей. Архивирование. Значение спецсредств. Криминалистические информационные системы. Компьютерные преступления. Криминалистическая характеристи-ка. 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
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Научно-исследовательская работа
2.1.2	Обеспечение безопасности современных серверов баз данных
2.1.3	Управление информационной безопасностью
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Безопасность вычислительных сетей
2.2.2	Интеллектуальные системы и технологии

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-2: Способен применять знания в области технологий и методов защиты информации при моделировании, разработке и документации систем защиты информации в автоматизированных системах
Знать:
технологии и методы обеспечения информационной безопасности; методы анализа и синтеза информационных систем при моделировании; разработку документации систем защиты информации в автоматизированных системах
Уметь:
технологии и методы обеспечения информационной безопасности; моделировать системы и разрабатывать документацию защиты автоматизированных систем
Владеть:
технологиями и мето дами обеспечения информационной безопасности; моделировать системы и разрабатывать документацию защиты автоматизированных систем

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	Компетен-ции	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-2	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-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.3	Криминалистические информационные системы. Компьютерные преступления. Криминалистическая характеристика. Статистика. /Лек/	4	2	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	

1.4	Личность вероятного преступника. Оперативность. Приоритетность расследования. /Лек/	4	2	ПК-2	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-2	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-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.7	Следственные действия. /Лек/	4	2	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
1.8	Компьютерно-техническая экспертиза. Перспективы. /Лек/	4	2	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
	Раздел 2. Лабораторные						
2.1	Перехват и исследование трафика /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.2	Исследование логов веб-сервера /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.3	Исследование системных логов /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.4	Исследование логов мейл-сервера и заголовков электронной почты /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.5	Установление принадлежности и расположения IP-адреса /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.6	Установление принадлежности доменного имени /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	2	Ситуационный анализ
2.7	Принадлежноть адреса электронной почты /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
2.8	Кейлогеры /Пр/	4	4	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
	Раздел 3. Самостоятельная работа						
3.1	Подготовка к лекциям /Ср/	4	8	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.2	Подготовка к практическим /Ср/	4	16	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.3	Расчетно-графические работы /Ср/	4	16	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
3.4	Подготока к зачету /Ср/	4	10	ПК-2	Л1.1Л2.1 Л2.2 Э1 Э2	0	
	Раздел 3.						

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, http://znanium.com/go.php?id=776078

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, http://biblioclub.ru/index.php?page=book&id=101046

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

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

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

1.Информационно-правовой портал КонсультантПлюс - http://www.consultant.ru

2.Профессиональные справочные системы Техэксперт - http://www.cntd.ru

3.Информационно-правовой портал Гарант.ру - http://www.garant.ru

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

Аудитория	Назначение	Оснащение
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
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 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

Аудитория	Назначение	Оснащение
		015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор.
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)

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. Принадлежноть адреса электронной почты
4. Кейлогеры

Отчет должен соответствовать следующим требованиям:
1. Отчет результатов РГР оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
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»
Реализация дистанционных занятий осуществляется в соответствии со СТ 02-02-18 "Реализация образовательных программ с использованием электронного обучения и дистанционных образовательных технологий".