МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.08
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Компьютерная криминалистика
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**6**	**Итого**
Форма контроля / **Вид занятий**	**зачет**	
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	48,75	48,75
Самостоятельная работа	95,75	95,75
Контроль		
Итого	**144**	**144**

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Цель дисциплины – изучения методов и средств проведения исследований в компьютерной криминалистике.

В процессе изучения основное внимание уделяется артефактам операционной системы, в частности ОС Windows, которые применяются при проведении криминалистических исследований. Так изучаются методы извлечения и получения данных артефактов. Особое внимание уделяется механизмам получения образов дисков и оперативной памяти исследуемых систем, программных и аппаратным средствам. Помимо этого, изучаются программные средства для анализа как образов, так и полученных из них артефактов.

Особое внимание уделяется расследованию компьютерных инцидентов.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Технологии и методы социальной инженерии;
- Информационная безопасность компьютерных сетей.

Полученные знания используются при изучении следующих дисциплин:

- Аудит защищенности информационных систем;
- Мониторинг событий информационной безопасности.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.5 Использует знание сетевых сервисов и протоколов, методов обнаружения атак на уровне сети, хостов и облаков, концепций и методологий анализа вредоносного ПО	Знать: -знание угроз и уязвимостей -знание законодательства (без уточнения какого) -знание категорий инцидентов -знание методов обнаружения атак на уровне сети, хостов и облаков -знание рисков безопасности приложений
		Уметь: -классификация и приоритизация инцидентов -документирование инцидента -оценка тенденций -анализ логов от разных источников -взаимодействие с правоохранительными или иными специальными органами, проводящими расследование инцидента -координация функций по реагированию на инциденты
		Владеть:

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		навыками обеспечения целостности цифровых доказательств на разных платформах и в соответствие с требованиями локального законодательства навыками защиты сетевых коммуникаций навыками распознавания и категоризации типов уязвимостей и связанных с ними атак навыками оценки ущерба
	ПК-6.6 Применяет навыки анализа логов от разных источников, корреляции данных по разным инцидентам, подготовки рекомендаций по их нейтрализации и сбора артефактов по инцидентам	Знать: - сетевые сервисы и протоколы; - основных сетевых концепций, включая топологии, протоколы, компоненты
		Уметь: - проводить сбор артефактов по инцидентам написание отчетов по инцидентам; - проводить -мониторинг внешних источников данных
		Владеть: - навыками защиты сети от вредоносного ПО
	ПК-6.7 Владеет навыками идентификации, получения, локализации и репортинга по вредоносному ПО, обеспечения целостности цифровых доказательств на разных платформах и в соответствие с требованиями локального законодательства	Знать: - знание концепции и методологии анализа вредоносного ПО
		Уметь: - производить корреляция данных по разным инцидентам и подготовка рекомендаций по их нейтрализации
		Владеть: - навыками использования средств корреляции событий ИБ; - навыками идентификации, получения, локализации и репортинга по вредоносному ПО

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Введение в форензику_1 1.Подразделы форензики. 2.Задачи форензики. 3.Общенаучные методы. 4.Актуальные атаки и известные 5.преступные группировки. 6.Основные источники данных. 7.Организационно-правовые аспекты. 8.Компьютерные преступления 9.Специальные технические средства	6	2		-	
Модуль 1	Ср	Тема 1 Введение в форензику_1	6	12			
Модуль 1	Лек	Тема 1 Введение в форензику_2 6.Основные источники данных. 7.Организационно-правовые аспекты. 8.Компьютерные преступления 9.Специальные технические средства	6	2		-	
Модуль 1	Ср	Тема 1 Введение в форензику_2	6	12			
Модуль 1	Лек	Тема 2 Артефакты системы 1.Таймлайны и источники. 2.Оперативно-розыскные мероприятия 3.Файловая система (NTFS). 4.Перехват и исследование трафика. 5.Реестр ОС. 6.Журнал событий Windows. 7.Используемые файлы. 8.История посещения браузеров	6	2		-	
Модуль 1	Пр	Тема 2 Артефакты системы Оформление документации по оперативно-розыскным мероприятиям	6	2			Отчет по практическому занятию №1
Модуль 1	Пр	Тема 2 Артефакты системы Перехват и исследование трафика с использованием	6	2			Отчет по практическому занятию № 2

		инструментария Kali Linux					
Модуль 1	Пр	Тема 2 Артефакты системы Анализ логов, системных журналов, файловой системы	6	2			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 2 Артефакты системы	6	12			
Модуль 1	Лек	Тема 3 Компьютерно-техническая экспертиза 1.Фреймворки 2.Методы КТЭ. 3.Работа с файловой системой. 4.Лог-файлы 5.Работа с реестром ОС. 6.Системная конфигурация. 7.Исследование программ. 8.Анализ журнала событий Windows. 9.Исследование дополнительных источников данных. 10.Активность пользовательских браузеров. 11. Поиск нестандартных процессов и подключений	6	2			
Модуль 1	Пр	Тема 3 Компьютерно-техническая экспертиза Анатомия атаки	6	4			Отчет по практическому занятию №4
Модуль 1	Пр	Тема 3 Компьютерно-техническая экспертиза Практика готовности к инцидентам	6	2			Отчет по практическому занятию №5
Модуль 1	Пр	Тема 3 Компьютерно-техническая экспертиза Выявление необычных служб и нестандартных подключений	6	2			Отчет по практическому занятию №6
Модуль 1	Ср	Тема 3 Компьютерно-техническая экспертиза	6	12			
Модуль 1	Лек	Тема 4 Практика экспертизы 1.Действия специалиста на месте инцидента	6	2			

		2.Следственные действия 3.Тактика обыска 4.Анализ заражённой системы на месте и его задачи. получение артефактов на месте инцидента. 5.Анализ снимка оперативной памяти. 6.Создание криминалистического образа накопителя 7. Удаление следов					
Модуль 1	Пр	Тема 4 Практика экспертизы Порядок сбора улик, действий специалиста	6	2			Отчет по практическому занятию №7
Модуль 1	Пр	Тема 4 Практика экспертизы Анализ зараженной системы	6	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 4 Практика экспертизы	6	12			
Модуль 1	Лек	Тема 5 Реагирование на инциденты_1 1.Готовность к инцидентам 2.Инструменты удаленной сортировки 3.Создание дампа памяти 4.Создание образа диска 5.Инструменты мониторинга сетевой безопасности 6.Анализ событий системы 7Анализ памяти 8.Анализ вредоносных программ	6	2		-	
Модуль 1	Ср	Тема 5 Реагирование на инциденты_1	6	12			
Модуль 1	Лек	Тема 5 Реагирование на инциденты_2 9.Извлечение информации с образа жесткого диска 10.Анализ дальнейшего распространения по сети 11. Выявление элементов инфраструктуры, затронутых инцидентом 12.Меры по сглаживанию последствий 13.Эмуляция действий злоумышленника 14. Взаимодействие с НКЦКИ	6	2			

Модуль 1	Пр	Тема 5 Реагирование на инциденты_2 Создание образа диска и образа виртуальных машин	6	4			Отчет по практическому занятию №9
Модуль 1	Ср	Тема 5 Реагирование на инциденты_2	6	11			
Модуль 1	Лек	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики	6				
Модуль 1	Пр	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Применение инструментов сетевой безопасности	6	4			Отчет по практическому занятию №10
Модуль 1	Ср	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики	6	11,75			
Модуль 1	Пр	Тема 6 Новые и развивающиеся технологии в области цифровой криминалистики Анализ действий вредоносных программ, обнаружение, нейтрализация	6	4			Отчет по практическому занятию №11
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно)	6	0,25		-	Банк тестовых заданий /Вопросы к зачету
			Итого:	**144**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-6	Протоколы практических заданий №1-11
		Вопросы к зачету №№1-45
		Темы для реферата
		Банк тестовых заданий №1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1.1 Реферат «Виды и методы атак на проникновение»
7.2.1.2 Реферат «Компьютерные преступления»
7.2.1.3 Реферат «Обзор DLP решений»
7.2.1.4 Реферат «Обзор техник компьютерной криминалистики»
7.2.1.5 Реферат «Методы исследования трафика»

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Оформление документации по оперативно-розыскным мероприятиям
2	Перехват и исследование трафика с использованием инструментария Kali Linux
3	Анализ логов, системных журналов, файловой системы
4	Анатомия атаки
5	Практика готовности к инцидентам
6	Выявление необычных служб и нестандартных подключений
7	Порядок сбора улик, действий специалиста
8	Анализ зараженной системы
9	Создание образа диска и образа виртуальных машин
10	Применение инструментов сетевой безопасности
11	Анализ действий вредоносных программ, обнаружение, нейтрализация

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты изучают сбор, анализ и интерпретация цифровых данных, включая оставленные следы на компьютере или в сети Интернет, расследование преступлений в области компьютерной безопасности,

включая методы анализа данных и процедуры судебного преследования, практические примеры и кейсы расследования цифровых преступлений.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.4. Типовой пример тестового задания

Объектом цифровой криминалистики являются:

Выберите один или несколько вариантов ответа:

1) правонарушения, связанные с использованием компьютерных технологий
2) общественные отношения, возникающие в ходе выявления нарушений
3) рабочие места пользователей
4) программное обеспечение

Критерии оценки:

Минимальное количество баллов 1. Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№ п/п	Вопросы к зачету
1.	Отличие форензики от аудита
2.	Форензика как наука о расследовании киберпреступлений
3.	Общенаучные и специальные методы форензики
4.	Понятие взлома в криминалистике
5.	Рассмотреть орудия и инструменты взлома
6.	Классифицировать следы взлома
7.	Перечислить методы фиксаций орудий и следов взлома
8.	Методы обнаружения вредоносных программ
9.	Методы распространения вредоносного программного кода

10.	Понятие оперативно розыскных мероприятий
11.	Журнал событий Windows
12.	Методы поиска субдоменов
13.	Действия специалиста на месте инцидента
14.	Понятие компьютерного инцидента
15.	Этапы компьютерной экспертизы
16.	Порядок восстановления хронологии (таймлайн) атаки
17.	Порядок сбора артефактов
18.	Методы и техники компьютерной экспертизы
19.	Привести примеры компьютерных преступлений
20.	Порядок исследования трафика, применяемое ПО
21.	Анализ лог файлов, применяемое ПО
22.	Какие вопросы стоят перед экспертом
23.	Средства и инструменты КТЭ
24.	Порядок исследования ПО
25.	Объекты исследования КТЭ
26.	Какие фрэймворки применяются для КТЭ и их возможности
27.	Отличие форензики от аудита
28.	Порядок аудита изменений конфигурации системы
29.	Порядок аудита процессов
30.	Порядок анализа жесткого диска
31.	Признаки работы вредоносных программ
32.	Защита целостности улик
33.	Меры предосторожности при работе с инцидентом ИБ
34.	Подозрительные учетные записи, службы, выявление, анализ
35.	Порядок использования PowerShell для запроса журналов событий
36.	Источники данных памяти
37.	Использование Volatility и Rekall
38.	Эмуляция действий злоумышленника
39.	Документирование результатов расследования
40.	Тактики и техники из техники MITRE ATT&CK
41.	Удаление следов процесса расследования
42.	Встроенные возможности Windows для аудита
43.	Сущность аппаратной форензики
44.	Сущность сетевой форензики
45.	Какие данные собираются из Windows

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Н.Н.Федотов	Форензика – компьютерная криминалистика	учебно-методическое пособие	2021	
2	О.И. Скулкин	Windows Forensics Cookbook	Учебное пособие	2022	
3	С.В. Паулевич	Форензик-экспертиза: сущность и основные методы организации финансовых расследований в компаниях	Журнал	2020	https:// cyberleninka.ru/ journal/n/vestnik-moskovskogo-universiteta-seriya-6-ekonomika?i=1082882

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Ю.Г. Горшков	Криминалистическое исследование	Учебное пособие	2019	https://

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		фонограмм			reader.lanbook.com/book/103620
2			Комментарии к Доктрине информационной безопасности Российской Федерации		2019

8.3. Перечень профессиональных баз данных и информационных справочных систем

Суханов М. Компьютерная контркриминалистика: состояние и перспективы [Электронный ресурс]. - Режим доступа: www.securitylab.ru/ana-lytics

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы	Столы, стулья,

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	обучающихся Г-401	компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф