МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

СОГЛАСОВАНО
Руководитель ОП

_____ Доброжинский Ю.В.
(подпись) (ФИО)

УТВЕРЖДАЮ
И.о. директора департамента информационной безопасности

_____ Боршевников А.Е.
(подпись) (Ф.И.О. Фамилия)
«03» __февраля__ 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы компьютерной криминалистики
Специальность 10.05.01 Компьютерная безопасность
(Безопасность компьютерных систем и сетей
(по отрасли или в сфере профессиональной деятельности)
Форма подготовки: очная

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459 (с изменениями и дополнениями).

Рабочая программа обсуждена на заседании департамента информационной безопасности, протокол № 5 от «03» февраля 2023 г.

И.о. директора департамента информационной безопасности: Боршевников А.Е.

Составители: Доцент Павлычев А.В.

Владивосток
2023

Оборотная сторона титульного листа РПД

1. Рабочая программа пересмотрена на заседании департамента информационной безопасности, протокол от «____» _____ 202 г. № _____

2. Рабочая программа пересмотрена на заседании департамента информационной безопасности, протокол от «____» _____ 202 г. № _____

3. Рабочая программа пересмотрена на заседании департамента информационной безопасности, протокол от «____» _____ 202 г. № _____

4. Рабочая программа пересмотрена на заседании департамента информационной безопасности, протокол от «____» _____ 202 г. № _____

Аннотация дисциплины

Основы компьютерной криминалистики

Общая трудоемкость дисциплины составляет 8 зачётных единиц / 288 академических часов. Является дисциплиной обязательной части ОП, изучается в течение двух семестров на 4 и 5 курсах, в качестве итогового испытания предусматриваются зачет и экзамен. Учебным планом предусмотрено проведение лекционных занятий в объеме 72 часов, практических занятий – 72 часов, а также выделены часы на самостоятельную работу студента – 144 часов.

Язык реализации: русский.

Для успешного изучения дисциплины у обучающихся должны быть сформированы следующие универсальные компетенции: владение компетенцией самосовершенствования (осознание необходимости, потребность и способность обучаться, способность к познавательной деятельности); умение применять соответствующий математический аппарат, приобретенные в результате получения среднего общего образования. Обучающийся должен быть готов к изучению таких дисциплин, как «Основы построения защищенных компьютерных сетей», «Защита в операционных системах», «Защита в операционных системах», «Основы построения защищенных баз данных», «Безопасность web-технологий» и других прикладных дисциплин.

Компетенции студентов, индикаторы их достижения и результаты обучения по дисциплине:

Код и наименование компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
ОПК-3 Способен контролировать уровень защищенности информационных систем и анализировать результаты аудитов информационных систем	ОПК-3.1 Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы компьютерной криминалистики» применяются следующие дистанционные образовательные технологии и методы активного/интерактивного обучения: видеоконсультация и обратная связь онлайн, индивидуальные консультации.

I. Цели и задачи освоения дисциплины:

Цель: получить знания и понимание основных аспектов компьютерной криминалистики.

Задачи:

- Получить понимание компьютерных преступлений: изучить различные виды компьютерных преступлений, их характеристики и методы совершения;
- Освоить стандарты и определения, используемые в компьютерной криминалистике;
- Освоить методы обнаружения и сбора доказательств компьютерных преступлений;
- Освоить методы исследования цифровых следов включая методы восстановления данных, анализа метаданных, криптографии;
- Изучить законодательные и правовые аспекты расследования компьютерных преступлений.

II. Трудоёмкость дисциплины и виды учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 4 зачётных единиц (144 академических часов).

Структура дисциплины:

Форма обучения – очная

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК*	СР	Контроль	
1	Раздел 1. Введение в компьютерную криминалистику	8	6	6			144		
2	Раздел 2. Классификация компьютерных	8	6	6					

	преступлений								
3	Раздел 3. Цифровые следы и их анализ	8	24	24					
4	Раздел 4. Законодательные и правовые аспекты	9	12	12					
5	Раздел 5. Технические средства и методы защиты от компьютерных преступлений	9	12	12					
6	Раздел 6. Этика и профессиональные стандарты	9	12	12					
	Итого:		72	72			144	27	

*онлайн курс

Ш. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел 1 - Введение в компьютерную криминалистику
Тема 1.1 - Определение компьютерной криминалистики и ее роль в борьбе с киберпреступлениями
Тема 1.2 - История развития компьютерных преступлений и криминалистики

Раздел 2 - Компьютерные преступления и их классификация
Тема 2.1 - Различные виды компьютерных преступлений, такие как хакерство, мошенничество, киберпреступления, нарушение авторских прав и др.
Тема 2.2 - Классификация компьютерных преступлений по характеристикам и методам совершения

Раздел 3 - Цифровые следы и их анализ
Тема 3.1 - Виды и источники цифровых следов, оставляемых при совершении компьютерных преступлений
Тема 3.2 - Методы сбора, фиксации и анализа цифровых следов
Тема 3.3 - Использование специализированных инструментов и программного обеспечения для анализа цифровых следов

Раздел 4 - Законодательные и правовые аспекты
Тема 4.1 - Законы и нормативные акты, регулирующие компьютерные преступления
Тема 4.2 - Правовые аспекты сбора, сохранения и использования электронных доказательств

Тема 4.3 - Судебные процедуры и требования при расследовании компьютерных преступлений

Раздел 5 - Технические средства и методы защиты от компьютерных преступлений
Тема 5.1 - Основы кибербезопасности и методы защиты информационных систем от угроз
Тема 5.2 - Разработка и реализация мер по предотвращению компьютерных преступлений
Тема 5.3 - Введение в методы обнаружения вторжений и мониторинга сетевого трафика

Раздел 6 - Этика и профессиональные стандарты
Тема 6.1 - Этические вопросы, связанные с компьютерной криминалистикой использованием электронных доказательств
Тема 6.2 - Профессиональные стандарты и ответственность в сфере компьютерной криминалистики

IV. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

Раздел 1

ЛАБОРАТОРНАЯ РАБОТА № 1. Анализ известных случаев компьютерных преступлений и изучение их влияния на общество.

ЛАБОРАТОРНАЯ РАБОТА №2. Исследование и дискуссия о ролях и ответственностях компьютерных криминалистов.

Раздел 2

ЛАБОРАТОРНАЯ РАБОТА № 3. Исследование различных видов компьютерных преступлений, их признаков и методов совершения через анализ реальных случаев.

ЛАБОРАТОРНАЯ РАБОТА № 4. Классификация компьютерных преступлений на основе их характеристик и последствий.

Раздел 3

ЛАБОРАТОРНАЯ РАБОТА № 5. Практическое знакомство с инструментами и программным обеспечением для сбора и анализа цифровых следов.

ЛАБОРАТОРНАЯ РАБОТА № 6. Анализ цифровых следов, оставленных на компьютере или в сетевом трафике, и выявление важных доказательств.

Раздел 4.

ЛАБОРАТОРНАЯ РАБОТА № 7. Исследование релевантных законодательных актов и нормативных документов, регулирующих компьютерные преступления.

ЛАБОРАТОРНАЯ РАБОТА № 8. Анализ и обсуждение решений судебных дел, связанных с компьютерной криминалистикой и использованием электронных доказательств.

Раздел 5

ЛАБОРАТОРНАЯ РАБОТА № 9. Создание и настройка виртуальной среды для тестирования уязвимостей и проведения практических атак.

ЛАБОРАТОРНАЯ РАБОТА № 10. Проектирование и реализация мер по обеспечению безопасности информационных систем, включая межсетевые экраны, IDS, WAF, применение криптографии.

Раздел 6

ЛАБОРАТОРНАЯ РАБОТА № 11. Обсуждение этических проблем, связанных с обработкой и использованием электронных доказательств.

ЛАБОРАТОРНАЯ РАБОТА № 12. Разработка кодекса этики для компьютерных криминалистов и обсуждение профессиональных стандартов.

V. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Код и наименование индикатора достижения	Оценочные средства *	
			текущий контроль	промежуточная аттестация

1	Разделы 1-3	ПК-3.1 Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети	УО-1 ЛР-6	-
2	Зачет			
3	Разделы 4-6	ПК-3.1 Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети	УО-1 ЛР-6	-
4	Экзамен			

* Формы оценочных средств:

1) собеседование/устный опрос (УО-1).
2) лабораторная работа (ЛР-6).

VI. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного

руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности.

Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности.

Формы самостоятельной работы студентов:

- работа с основной и дополнительной литературой, интернет-ресурсами;

- самостоятельное ознакомление с лекционным материалом, представленным на электронных носителях, в библиотеке образовательного учреждения;

- выполнение лабораторных работ;

- подготовка к зачету и экзамену;

- другие виды деятельности, организуемые и осуществляемые образовательным учреждением и органами студенческого самоуправления.

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы компьютерной криминалистики» включает в себя план-график выполнения самостоятельной работы по дисциплине.

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля

1.	В течение первого семестра	Изучение литературы, подготовка к лабораторным работам. Подготовка к сдаче зачета	72 час	УО-1ПР-6
2.	В течение второго семестра	Изучение литературы, подготовка к лабораторным работам. Подготовка к сдаче экзамена	72 час	УО-1 ПР-6
	Итого		144 час	

Самостоятельная работа по дисциплине включает в себя подготовку к лабораторным занятиям (изучение литературы) и подготовку к промежуточной аттестации по дисциплине.

Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ (http://www.dvfu.ru/library/) и других ведущих вузов страны, а также доступных для использования научно-библиотечных систем.

VII. СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Компьютерная криминалистика (Михаил Козаченко)
2. Компьютерная криминалистика (Алексей Никитин, Евгений Кузьминых)
3. Основы компьютерной криминалистики (Андрей Кулагин, Александр Пестунов)
4. Компьютерная криминалистика: Полный курс (Юрий Сорокин)
5. Компьютерная криминалистика: Анализ и судебно-экспертное исследование (Александр Макаров)
6. Компьютерные преступления: Уголовно-правовой и криминалистический аспекты (Игорь Расторгуев)
7. Компьютерные преступления и кибербезопасность (Сергей Басенко)
8. Компьютерная криминалистика: Методы и проблемы (Иван Алексеев)

9. Компьютерные преступления и информационная безопасность (Евгений Макаров, Валерий Розин)

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

0. Статьи на портале SecurityLab: https://www.securitylab.ru/
1. Статьи на портале Xakep: https://xakep.ru/
2. Бесплатный курс форензики: https://www.cybrary.it/course/computer-hacking-forensics-analyst
3. Форензика в Android: https://opensecuritytraining.info/AndroidForensics.html
4. Тестирование: https://www.skillset.com/skills/computer-forensics-fundamentals
5. Образцы дампов памяти для анализа: https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
6. Образцы дампов трафика для анализа: https://wiki.wireshark.org/SampleCaptures
7. Образцы для тренировки в форензике: https://cfreds.nist.gov/
8. Тематический WEB-ресурс https://digitalcorpora.org/

Перечень информационных технологий и программного обеспечения

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение: Microsoft Teams, Microsoft Office программное обеспечение сервисов сайта ДВФУ, включая ЭБС ДВФУ.

Информационно справочные системы и профессиональные базы данных:

1. ЭБС ДВФУ - https://www.dvfu.ru/library/electronic-resources/
2. Электронная библиотечная система «Лань»: https://e.lanbook.com/
3. Электронная библиотечная система «Консультант студента»: http://www.studentlibrary.ru
4. Электронная библиотечная система «eLIBRARY.RU»: http://www.elibrary.ru/
5. Электронная библиотечная система «Юрайт»: http://www.urait.ru/ebs

6. Электронная библиотечная система «Znanium»: http://znanium.com/

7. Электронная библиотечная система IPRbooks: http://iprbookshop.ru/

8. Электронная библиотека диссертаций Российской государственной библиотеки http://diss.rsl.ru/

9. База данных Scopus http://www.scopus.com/home.ur0l

10. База данных Web of Science http://apps.webofknowledge.com/

11. Информационная система "ЕДИНОЕ ОКНО доступа к образовательным ресурсам" - http://window.edu.ru/

12. Доступ к электронному заказу книг в библиотеке ДВФУ - http://lib.dvfu.ru:8080/search/query?theme=FEFU

VIII. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекциях и лабораторных занятиях, выполнение аттестационных мероприятий. В процессе изучения дисциплины студенту необходимо ориентироваться на проработку лекционного материала, подготовку к лабораторным занятиям.

дисциплины «Основы компьютерной криминалистики» предполагает рейтинговую систему оценки знаний студентов и предусматривает со стороны преподавателя текущий контроль за посещением студентами лекций, лабораторных занятий, выполнением всех видов заданий и самостоятельной работы.

Студент считается аттестованным по дисциплине при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Шкала оценивания сформированности образовательных результатов по дисциплине представлена в фонде оценочных средств (ФОС).

IX. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине проводятся в помещениях, оснащенных соответствующим оборудованием и программным обеспечением.

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещенийи помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. – компьютерный класс. Компьютерный класс для проведения занятий с проектором, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: проектор и ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная.	Autopsy: Бесплатная и открытая среда цифрового расследования, которая позволяет анализировать цифровые следы, извлекать информацию и восстанавливать удаленные файлы. EnCase Forensic: Мощное программное обеспечение для цифрового расследования и анализа данных, которое широко используется в области компьютерной криминалистики. X-Ways Forensics: Программное обеспечение для цифрового расследования, которое обеспечивает широкие возможности анализа данных, включая восстановление удаленных файлов, анализ файловой системы и др. Cellebrite UFED: Инструмент для физического и логического извлечения данных с мобильных устройств, который может быть полезен при анализе мобильных телефонов и планшетов. Wireshark: Мощный инструмент для анализа сетевого трафика, который может использоваться для обнаружения атак, исследования взаимодействия сетевых устройств и анализа сетевых протоколов. Volatility: Инструментарий для анализа памяти компьютера, который позволяет извлекать информацию из дампов памяти и анализировать процессы и данные в оперативной памяти.
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус A, ауд. – 1042. Аудитория для самостоятельной работы студентов	Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскопечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео	

	увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой.	Oxygen Forensic Detective: Программное обеспечение для мобильной форензики, которое позволяет извлекать данные с мобильных устройств и анализировать их, включая извлечение информации из социальных сетей и мессенджеров. Palisade's Enforcer: Инструмент для обнаружения вредоносных программ и сетевых атак, который позволяет обнаруживать и реагировать на угрозы информационной безопасности. AccessData FTK: Программное обеспечение для цифрового расследования и анализа данных, которое обладает широкими возможностями для извлечения и анализа цифровых следов. Hashcat: Утилита для восстановления паролей, которая может быть полезна при анализе зашифрованных данных и паролей.