Рабочая программа дисциплины (модуля)*
Компьютерная криминалистика (научный семинар)

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2025

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2025г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки.

УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.

ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о методах анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно- технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов.

ПК-1.2. Демонстрирует умения: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов.

ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения причин и условий изменения свойств исследуемой информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.01.06

2.1 Требования к предварительной подготовке обучающегося:

Основы информационной безопасности

Сбор данных из открытых источников (научный семинар)

Системы управления базами данных

Компьютерные сети

Основы построения защищенных компьютерных сетей

Основы построения защищенных баз данных

Беспроводные сети

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Знать:

– основы выполнения эффективного поиска информации;
– алгоритмы расследований инцидентов информационной безопасности.

Уметь:

– определять критерии системного анализа для поставленных задач;
– проводить компьютерно-технические экспертизы.

Владеть:

– навыками системного анализа и поиска информации.

ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов

Знать:

– технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов.

Уметь:

– применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа.

Владеть:

– составления экспертного заключения;
– установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основы компьютерной криминалистики;
3.1.2	– правовые нормы расследований инцидентов информационной безопасности;
3.1.3	– алгоритмы расследований инцидентов информационной безопасности.
3.2	**Уметь:**
3.2.1	– самостоятельно проводить расследования инцидентов информационной безопасности;
3.2.2	– проводить компьютерно-техническую экспертизу.
3.3	**Владеть:**
3.3.1	– поиска цифровых следов в компьютерных системах;
3.3.2	– фиксации следов в компьютерных системах в качестве доказательств в гражданских и уголовных делах;
3.3.3	– анализировать собранные материалы с целью выявления источника атаки и восстановления работоспособности системы;
3.3.4	– документировать противоправные действия злоумышленника.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**6 ЗЕТ**
Часов по учебному плану : 216 в том числе : аудиторные занятия : 68 самостоятельная работа : 101 часов на контроль : 36 контактная работа: 79 ИКР: 11	Виды контроля в семестрах: экзамены 10

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основы компьютерной криминалистики			

1.1	Введение в компьютерную криминалистику. Специальность – компьютерный криминалист. Особенности современных подходов: Windows криминалистика, криминалистика оперативной памяти, криминалистика мобильных устройств, криминалистика сетевого траффика. /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
1.2	Введение в компьютерную криминалистику. Специальность – компьютерный криминалист. Особенности современных подходов: Windows криминалистика, криминалистика оперативной памяти, криминалистика мобильных устройств, криминалистика сетевого траффика. /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
1.3	Особенности современных подходов: Windows криминалистика, криминалистика оперативной памяти, криминалистика мобильных устройств, криминалистика сетевого траффика. /Ср/	10	4	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 2. Документирование оперативной памяти			
2.1	Хищения у юридических лиц Хищения у физических лиц Целенаправленные атаки на банки и финансовые организации Технические аспекты атак: методы распространения, мошенничества с банковскими картами, СИМ-картами, подмена платежные поручений и т.д. /Лек/	10	6	Л1.1 Л1.2Л2.1 Л2.2
2.2	Хищения у юридических и у физических лиц. Технические аспекты атак. /Пр/	10	6	Л1.1 Л1.2Л2.1 Л2.2
2.3	Хищения у юридических и у физических лиц. Технические аспекты атак. /Ср/	10	20	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 3. Документирование НЖМД			
3.1	Безопасность электронной почты Безопасность паролей Безопасность мобильный приложений Безопасность компьютеров Безопасность браузеров Безопасность соц. Сетей /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
3.2	Безопасность электронной почты Безопасность паролей Безопасность мобильный приложений Безопасность компьютеров Безопасность браузеров Безопасность соц. Сетей /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
3.3	Цифровая гигиена /Ср/	10	15	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 4. Анализ сетевого трафика			
4.1	Терминология в области ИБ Риск-ориентированный подход к обеспечению ИБ в Организации CIS Controls /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
4.2	Терминология в области ИБ Риск-ориентированный подход к обеспечению ИБ в Организации CIS Controls /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
4.3	Терминология в области ИБ Риск-ориентированный подход к обеспечению ИБ в Организации CIS Controls /Ср/	10	15	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 5. Стеганография			
5.1	Эволюция атак группировки Cobalt Strike Атака изнутри: инструменты, методы атак, технологии /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
5.2	Имитация атак /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2

5.3	Имитация атак /Ср/	10	15	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 6. Реагирование на инциденты ИБ. Правовая база расследований киберпреступлений			
6.1	Построение команды по реагированию на инциденты ИБ Дорожная карта при реагировании на инциденты ИБ Правовая база расследования киберпреступлений /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
6.2	Реагирование на инциденты ИБ /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
6.3	Реагирование на инциденты ИБ /Ср/	10	15	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 7. Правовые основы СКТЭ			
7.1	Криптоиндустрия: новое направление – «старые» угрозы Основные участники и риски Безопасность криптопроектов /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
7.2	Безопасность криптопроектов /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
7.3	Безопасность криптопроектов /Ср/	10	10	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 8. Практическая форензика			
8.1	Поиск с помощью порталов и сайтов организаций Поиск с помощью государственных информационных ресурсов Поиск с помощью социальных сетей Иные источники информации /Лек/	10	4	Л1.1 Л1.2Л2.1 Л2.2
8.2	Поиск информации по открытым источникам /Пр/	10	4	Л1.1 Л1.2Л2.1 Л2.2
8.3	Поиск информации по открытым источникам /Ср/	10	7	Л1.1 Л1.2Л2.1 Л2.2
	Раздел 9. Иная контактная работа			
9.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	10	11	Л1.1 Л1.2Л2.2

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Аудиторные задания.
Перечень вопросов к экзамену.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Аудиторные задания:
1 Снятие образа диска, образ RAM, как правильно запускать виртуальные машины (без интернета и прочее).
2. Документирование НЖМД (linux, windows)
3. Анализ сетевого трафика
4. Стеганография
5. Проведение типовой СКТЭ

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену (практические):
1 Снятие образа диска, образ RAM, как правильно запускать виртуальные машины (без интернета и прочее).
2. Документирование НЖМД (linux, windows)
3. Анализ сетевого трафика
4. Проведение типовой СКТЭ

Вопросы к экзамену (теоретические):
1. Уголовно-правовая характеристика преступлений, совершенных с использованием информационных, коммуникационных технологий.
2. Проблемы квалификации и отличия статей УК РФ: п. В ч. 3 ст. 158, ст.159.3, ст. 159.6 и 159 УК.
3. Проблемы квалификации и отличия статей УК РФ: 272, ст.273, ст. 274.

4. Криминалистическая характеристика преступлений в платежных системах. Способы установления субъектов и оборудования платежных систем в криминальной деятельности.
5. Криминалистическая характеристика преступлений с использованием IP-телефонии. Способы и методы вычисления лиц использующих при совершении преступлений iP-телефонии.
6. Технико-криминалистическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий.
7. Криминалистическая характеристика преступлений в сфере компьютерной информации.
8. Особенности расследования преступлений в сфере компьютерной информации. тактико-технические
9. Использование специальных технических знаний в оперативно-розыскной деятельности.
10. Использование специальных знаний при расследовании преступлений в сфере информационных технологий.
11. Участие специалиста при проведении следственных действий в отношении средств вычислительной техники и программного обеспечения. Основы назначения судебных компьютерных экспертиз. Особенности проведения судебных компьютерных экспертиз.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
В течение семестра студентам необходимо выполнить одну самостоятельную работу, которая в случае безупречного выполнения оценивается в 80 баллов.
Кроме того, в рамках зачета студентам предлагается 2 вопроса, каждый из которых оценивается в 10 баллов.

Сводная таблица рейтинга успеваемости

Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
Экзамен (практический вопрос)	80
Экзамен (теоретический вопрос)	2x10=20
Итого	100

Критерии оценивания теоретического вопроса
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и грамотно сформулировать доказательство.
Хорошо/ зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом, но допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-4 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими и ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания практического задания
Каждое задание самостоятельной работы оценивается от 0 до 10 баллов, соответствие требованиям оформления оценивается от 0 до 10 баллов.
Максимальный балл за работу – 80 баллов.
Отлично/зачтено/70-80 баллов - Работа выполнена в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.
Хорошо/зачтено/60-69 баллов - Работа выполнена в срок, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/41-59 баллов - Работа выполнена и сдана позднее, чем предполагалось, и при этом обучающийся знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу. Обучающийся допускает незначительные ошибки.
Неудовлетворительно/не зачтено/0-40 баллов - Выполнены отдельные части работы, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

При подведении итогов не учитываются результаты текущей аттестации.
0-60 баллов - неудовлетворительно (2);
61-74 баллов - удовлетворительно (3);
75-90 баллов - хорошо (4);
91-100 баллов - отлично (5).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Яблоков Н.П.	Криминалистика в вопросах и ответах: учебное пособие (https://znanium.com/catalog/document?id=358554)	Москва : ООО "Юридическое издательство Норма", 2020	ЭБС
Л1.2	Яблоков Н.П., Головин А. Ю.	Криминалистика: природа, система, методологические основы: монография (https://znanium.com/catalog/document?id=380028)	Москва : ООО "Юридическое издательство Норма", 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1		Компьютерная криминалистика: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=466995)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017	ЭБС
Л2.2	Грибунин В. Г., Оков И. Н., Туринцев И. В.	Цифровая стеганография: учебное пособие (https://biblioclub.ru/index.php?page=book&id=117549)	Москва : СОЛОН-ПРЕСС, 2009	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

LMS Moodle

Adobe Connect Acrobat

Android Studio

Dev C++

Java Development Kit

Notepad++

Python

Arduino IDE

LibreOffice

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях рассматриваются виды преступлений в сфере компьютерной информации, методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем. Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.
Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.
При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Специальность 10.05.01 Компьютерная безопасность
Специализация № 1 «Анализ безопасности компьютерных систем»
Рабочая программа дисциплины «Компьютерная криминалистика (научный семинар)»
2025 год набора, очная форма обучения

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1