Рабочая программа дисциплины (модуля)*

Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 6 "Информационно-аналитическая и техническая экспертиза 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 2025 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка специалиста, владеющего технологиями выявления следов компьютерных преступлений, совершаемых с использованием новых информационных технологий, способного применять эти знания и навыки в рамках дальнейшей его практической деятельности.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-6.1.1.1. Знает основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;

ОПК-6.1.1.2. Знает методы и средства сбора и обращения с доказательными данными.

ОПК-6.1.2.1. Умеет определять причины, цели и условия изменения свойств (состояния) программного обеспечения;

ОПК-6.1.2.2. Умеет обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.32.03

2.1 Требования к предварительной подготовке обучающегося:

Экспертиза вычислительной техники и компьютерных носителей информации

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

Основы компьютерной криминалистики

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

ОПК-6.1: Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;

Знать:

– основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;
– методы и средства сбора и обращения с доказательными данными.

Уметь:

– определять причины, цели и условия изменения свойств (состояния) программного обеспечения;
– обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных.

Владеть:

– способами правильного установления, фиксации и оценки следов компьютерных преступлений и инцидентов.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– виды и типы компьютерных преступлений, этапы и методы проведения расследования компьютерных преступлений;
3.1.2	– методы и средства сбора и обращения с доказательными данными;
3.1.3	– правила установления лиц, причастных к совершению компьютерного преступления.
3.2	**Уметь:**
3.2.1	– выявлять факты, место и время неправомерного доступа к информации в компьютерной системе или сети;
3.2.2	– устанавливать надежность средств защиты компьютерной информации;
3.2.3	– выявлять способы несанкционированного доступа;

3.2.4	– осуществлять сбор доказательной базы и обстоятельств, способствовавших совершению преступления;
3.2.5	– устранять последствия преступления, осуществлять разработку и предоставление рекомендаций по минимизации рисков.
3.3	**Владеть:**
3.3.1	– выявления следов компьютерных преступлений;
3.3.2	– проведения основных этапов расследования компьютерных преступлений, правонарушений и инцидентов.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану : 144 в том числе : аудиторные занятия : 68 самостоятельная работа : 38 часов на контроль : 27 контактная работа: 79 ИКР: 11	Виды контроля в семестрах: экзамены 9

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Виды и типы компьютерных преступлений			
1.1	Вводная лекция. Обзор статей УК РФ по компьютерным преступлениям. /Лек/	9	6	Л1.1Л2.1 Л2.2
	Раздел 2. Выявление фактов, мест и времени неправомерного доступа к информации в компьютерной системе или сети			
2.1	Методы выявления неправомерного доступа к информации в компьютерной системе или сети. /Лек/	9	12	Л1.1Л2.1 Л2.2
2.2	Практическая работа. Настройка средств сбора логов. Установка коллекторов систем мониторинга. /Пр/	9	8	Л1.1Л2.1 Л2.2
2.3	Практическая работа. Установка средств сетевого мониторинга (IDS). /Пр/	9	6	Л1.1Л2.1 Л2.2
2.4	Сборки стендов с различными системами мониторинга. /Ср/	9	20	Л1.1Л2.1 Л2.2
	Раздел 3. Установление надежности средств защиты компьютерной информации			
3.1	Методы проверки надежности средств защиты. /Лек/	9	4	Л1.1Л2.1 Л2.2
3.2	Практическая работа. Readteaming инфраструктуры. /Пр/	9	4	Л1.1Л2.1 Л2.2
	Раздел 4. Выявление способов несанкционированного доступа			
4.1	Использование средств мониторинга в целях выявления несанкционированного доступа. /Лек/	9	4	Л1.1Л2.1 Л2.2
4.2	Практическая работа. Выявления признаков несанкционированного доступа. /Пр/	9	4	Л1.1Л2.1 Л2.2
	Раздел 5. Правила установления лиц, причастных к совершению компьютерного преступления			
5.1	Законодательная и практическая база по установлению лиц, причастных к инциденту ИБ. /Лек/	9	4	Л1.1Л2.1 Л2.2
5.2	Практическая работа. Анализ артефактов совершенного компьютерного преступления, использование OSINT- технологий. /Пр/	9	4	Л1.1Л2.1 Л2.2
	Раздел 6. Сбор доказательной базы и обстоятельств, способствовавших совершению преступления			
6.1	Расследование инцидента (преступления), разбор кейсов. /Пр/	9	4	Л1.1Л2.1 Л2.2

6.2	Самостоятельный разбор инцидента. /Ср/	9	18	Л1.1Л2.1 Л2.2
	Раздел 7. Устранение последствий преступления, разработка и предоставление рекомендаций по минимизации рисков			
7.1	Методы оценки нанесенного ущерба, выработка рекомендации, методики оценки рисков. /Лек/	9	4	Л1.1Л2.1 Л2.2
7.2	Практическая работа. Составление шаблона отчета. /Пр/	9	4	Л1.1Л2.1 Л2.2
	Раздел 8. Иная контактная работа			
8.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	9	11	Л1.1Л2.1 Л2.2

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Практическая работа.
Письменный опрос.
Перечень вопросов к экзамену.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Типовая практическая работа №1:
Настроить систему обнаружения вторжений на стендовый сетевой периметр.

Типовая практическая работа №2:
Настроить коллектор логов на стендовой инфраструктуре.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к экзамену

Как снимать образы объектов?
Как разворачивается экспертный стенд для исследований?
Состав экспертного стенда для исследований.
Какими ФЗ и иными нормативными актами регулируется деятельность эксперта?
Форма и состав отчета эксперта.
Порядок назначения и исполнения экспертизы или исследования СПО, используемое при исследованиях и границы его применения.
Порядок участия специалиста в следственных действиях.
Допрос эксперта.
Методики проведения исследований.

6.4. Критерии оценивания

В течение семестра предполагается проведение 6 практических работ на практических занятиях, и проведение 3 письменных опросов. В конце семестра планируется проведение экзамена. Допуском к экзамену являются 6 отчетов по практическим работам.
На экзамене студенту предлагается билет с 2 теоретическими вопросами.

Сводная таблица рейтинга успеваемости

Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
Практическая работа (отчет)	6х6 б=36 б
Письменный опрос	3х5 б=15 б
Экзамен (2 теор.вопроса)	2х5 б.=10 б.
Итого	61

Критерии оценивания письменного опроса
Максимальный балл за письменный опрос – 5 баллов.

Характеристики ответа	Баллы	Уровень освоения проверяемых компетенций
Правильно даны все пять ответов	5	высокий
Правильно даны четыре ответа	4	средний
Правильно даны три ответа	4	
Правильно даны два ответа	3	базовый
Правильно дан один ответ	3	
Нет правильных ответов	2	недостаточный

Критерии оценивания отчетов по темам практических занятий
Максимальный балл за практическую работу – 6 баллов.
Зачтено/6 баллов - Задания выполнены полностью и в срок, обучающийся отлично знает материал, и свободно отвечает на контрольные вопросы.
Зачтено/4-5 баллов - Задание выполнено полностью и в срок, обучающийся хорошо знает материал, грамотно излагает его, но при этом допускаются незначительные ошибки.
Зачтено/1-3 балла - Задание выполнено частично и/или сдано с опозданием. Обучающийся знаком с материалом, но допускает значительные ошибки, не оперирует основной терминологией и понятийным аппаратом по теме.
Не зачтено/0 баллов - Задание не выполнено, либо предоставлено с большим опозданием. Обучающийся не знает основных положений темы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания теоретического вопроса экзамена
Максимальный балл за ответ на теоретический вопрос – 5 баллов.
Отлично/зачтено/5 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/4 балла - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/3 балла - Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-2 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:
0-36 баллов – неудовлетворительно (2);
37-45 баллов – удовлетворительно (3);
46-54 баллов – хорошо (4);
55-61 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	Таненбаум Э., Леонтьев А.	Современные операционные системы	Санкт- Петербург : Питер, 2005	

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	Крылов В. В.	Информационные компьютерные преступления: учебное и практическое пособие	Москва : ИНФРА*М-НОРМА, 1997	

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

VirtualBox
Ubuntu Linux
LibreOffice
Python 3.7

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.

Лабораторные занятия проходят в учебных лабораториях технических средств защиты информации и "Сетевой полигон" (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.

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

1. Аппаратно-программный комплекс для исследования и восстановления поврежденных носителей данных (например, HDD PC-3000 Express).

2. Аппаратно-программный комплекс для криминалистического исследования фонограмм (например, ИКАР Лаб II+).

3. ЖК-монитор (например, DELL UP3216Q).

4. ЖК-телевизор (например, LG55UF680V).

5. Комплект акустических систем (например, JBL LSR305).

6. Устройство для копирования информации с компьютерных носителей с возможностью блокирования операций записи (напрмер, TabIeau T8-R2).

7. Устройство для копирования информации с компьютерных носителей с возможностью блокирования операций записи (апример, Tableau OEM T3iu).

8. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин.

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

При изучении данной дисциплины используются лекционные, лабораторные 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 основные методы проведения расследования компьютерных преступлений, правонарушений и инцидентов, методы и средства сбора и обращения с доказательными данными. Рекомендуется перед каждым практическим занятием выполнить полностью или частично текущее практическое

задание, что позволит на самом занятии уделить больше времени на отчёт преподавателю.

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 №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Рабочая программа дисциплины «Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов»
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