# Рабочая программа дисциплины (модуля)*
# Компьютерная безопасность

Направление подготовки (специальность)

44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль)

Экономика и информатика

Присваиваемая квалификация (степень)

бакалавр

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 изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления.

Задачи дисциплины:

– изучение основных аспектов обеспечения информационной безопасности государства;

– изучение методологии создания систем защиты информации;

– изучение процессов сбора, передачи и накопления информации;

– изучение основных элементов теории компьютерной безопасности;

– изучение математических основ моделей безопасности;

– изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ПК-2.1. Реализует современные формы и методы воспитательной работы непосредственно на учеб-ных занятиях и во внеурочной деятельности.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

| Цикл (раздел) ОПОП: | К.М.07.39 |
|---|---|

**2.1 Требования к предварительной подготовке обучающегося:**

Методы и средства защиты информации

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

Управление персоналом и кадровая безопасность

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

**ПК-2: Способен осваивать и использовать базовые научно-теоретические знания и практические умения по предмету в профессиональной деятельности**

**Знать:**

– содержание, сущность, закономерности, особенности изучаемых явлений и процессов, базовые теории в предметной области;
– принципы, определяющие место предмета в общей картине мира;
– основы данной дисциплины в объеме, необходимом для решения педагогических, научно- методических и организационно-управленческих задач.

**Уметь:**

– оценивать угрозы информационной и компьютерной безопасности в профессиональной деятельности;
– формировать собственные мнения по изучаемым проблемам, аргументировать свою позицию.

**Владеть:**

– основами реализации научно-теоретических знаний в области компьютерной безопасности в профессиональной деятельности.

**В результате освоения дисциплины обучающийся должен**

| | |
|---|---|
| **3.1** | **Знать:** |
| 3.1.1 | – сущность и понятие информации, информационной безопасности и характеристику ее составляющих; |
| 3.1.2 | – основы государственной информационной политики, стратегию развития информационного общества в России. |
| **3.2** | **Уметь:** |
| 3.2.1 | – пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; |
| 3.2.2 | – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. |
| **3.3** | **Владеть:** |

| | |
|---|---|
| 3.3.1 | – навыками использования профессиональной терминологии в области информационной безопасности; |
| 3.3.2 | – навыками построения систем защиты информации. |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

| | |
|---|---|
| Общая трудоемкость | **4 ЗЕТ** |
| Часов по учебному плану : 144<br>в том числе :<br>аудиторные занятия : 44<br>самостоятельная работа : 64,4<br>часов на контроль : 27<br>контактная работа: 52,6<br>ИКР: 8,6 | Виды контроля в семестрах:<br><br>экзамены 9 |

## 5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр / Курс | Часов | Литература |
|---|---|---|---|---|
| | **Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации** | | | |
| 1.1 | Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 1.2 | Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 1.3 | Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче экзамена. /Ср/ | 9 | 10 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| | **Раздел 2. Виды защищаемой информации ограниченного доступа** | | | |
| 2.1 | Организационно-правовой режим защиты государственной тайны. Организационно-правовой режим защиты коммерческой тайны. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 2.2 | Законодательство о персональных данных. Требования к защите ПД при их обработке в ИСПД. Виды угроз безопасности ПД при их обработке в ИСПД. Методика определения актуальных угроз безопасности ПД. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 2.3 | Виды защищаемой информации ограниченного доступа. Законодательство о персональных данных. /Пр/ | 9 | 4 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 2.4 | Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче экзамена. /Ср/ | 9 | 12 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| | **Раздел 3. Основы государственной политики Российской Федерации в области информационной безопасности** | | | |

| | | | | |
|---|---|---|---|---|
| 3.1 | Национальные интересы Российской Федерации в информационной сфере.<br>Виды и источники угроз информационной безопасности.<br>Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере.<br>Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 3.2 | Национальные интересы Российской Федерации в информационной сфере.<br>Виды и источники угроз информационной безопасности Российской Федерации.<br>Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере.<br>Организационная система обеспечения информационной безопасности Российской Федерации. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 3.3 | Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности.<br>Уголовно-процессуальная характеристика компьютерных преступлений. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 3.4 | Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности.<br>Уголовно-процессуальная характеристика компьютерных преступлений. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 3.5 | Проработка лекционного материала и литературы.<br>Подготовка выступлений на практических занятиях.<br>Подготовка к сдаче экзамена. /Ср/ | 9 | 12,4 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| | **Раздел 4. Информационное противоборство, методы и средства его осуществления** | | | |
| 4.1 | Понятие информационного противоборства.<br>Информационные войны, методы и средства их ведения.<br>Информационное оружие, его классификация и возможности.<br>Технические каналы утечки защищаемой информации. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 4.2 | Понятие информационного противоборства.<br>Информационные войны, методы и средства их ведения.<br>Информационное оружие, его классификация и возможности. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| 4.3 | Проработка лекционного материала и литературы.<br>Подготовка выступлений на практических занятиях.<br>Подготовка к сдаче экзамена. /Ср/ | 9 | 15 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 |
| | **Раздел 5. Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры** | | | |
| 5.1 | Общая характеристика методов и средств защиты информации в автоматизированных информационных системах /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.2 | Стратегические цели и основные направления.<br>Принципы и общие методы обеспечения обеспечения информационной безопасности.<br>Автоматизированная информационная система как объект защиты. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.3 | Стратегические цели и основные направления.<br>Принципы и общие методы обеспечения обеспечения информационной безопасности.<br>Автоматизированная информационная система как объект защиты. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |

| | | | | |
|---|---|---|---|---|
| 5.4 | Понятие комплексного обеспечения информационной безопасности. Политика обеспечения информационной безопасности предприятия (организации). /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.5 | Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.6 | Понятие комплексного обеспечения информационной безопасности. Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем. /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.7 | Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. /Лек/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.8 | Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общая характеристика методов и средств защиты информации в автоматизированных информационных системах. /Пр/ | 9 | 4 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.9 | Задачи и организационная структура подразделения обеспечения информационной безопасности предприятия (организации). /Пр/ | 9 | 2 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| 5.10 | Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче экзамена. /Ср/ | 9 | 15 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |
| | **Раздел 6. Иная контактная работа** | | | |
| 6.1 | Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/ | 9 | 8,6 | Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Перечень видов оценочных средств

Перечень вопросов к экзамену.
Перечень вопросов устного опроса.

### 6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса на практических занятиях.
1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы, угрозы национальной безопасности Российской Федерации.
3. Понятие информационной безопасности, основные составляющие национальных интересов в информационной сфере.
4. Факторы, способствующие повышению роли информационной безопасности в системе национальной безопасности.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности.
6. Компетенция федеральных и региональных органов государственной власти в сфере обеспечения информационной безопасности.
7. Правовая и организационная система обеспечения информационной безопасности Челябинской области.
8. Интересы личности общества и государства в информационной сфере.
9. Характеристика основных видов угроз информационной безопасности.
10. Принципы обеспечения информационной безопасности.
11. Понятие информационной войны, цели и средства её ведения.
12. Основные компоненты информационной войны.
13. Понятие информационного оружия.
14. Классификация информационного оружия.
15. Понятие и свойства информации.
16. Виды защищаемой информации.
17. Обязанности обладателя по обеспечению защиты информации.
18. Режим конфиденциальности информации и порядок его введения, на примере режима коммерческой тайны
19. Конституция Российской Федерации о правах и обязанностях граждан в информационной сфере.

20. Структура законодательства в сфере обеспечения информационной безопасности.
21. Перечень статей УК РФ, предусматривающих уголовную ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
22. Федеральные органы, осуществляющие контрольные функции в сфере обеспечения информационной безопасности.
23. .Административная ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
24. Понятие автоматизированной информационной системы.
25. Виды угроз безопасности информационных и телекоммуникационных систем.
26. Основные каналы утечки защищаемой информации.
27. Внешние источники угроз безопасности информационных систем.
28. Внутренние источники угроз безопасности информационных систем.
29. Элементы обстановки на объекте защиты, процедура оценки обстановки.
30. Критерии оценки защищенности автоматизированных информационных систем.
31. Структура службы безопасности предприятия.
32. Основные этапы создания службы безопасности предприятия.
33. Основные задачи, решаемые подразделением обеспечения информационной безопасности.
34. Обязанности руководителя подразделения информационной безопасности.
35. Обязанности системного администратора (администратора безопасности).
36. Обязанности пользователя автоматизированной информационной системы по обеспечению информационной безопасности.
37. Понятие и основные виды терроризма.
38. Роль информационных технологий в управлении критически важными объектами государства.
39. Способы совершения террористического акта в отношении объектов информационной инфраструктуры.
40. Использование террористическими организациями сети Интернет.
41. Понятие объекта, критически важного для обеспечения национальной безопасности государства, классификация критически важных объектов.
42. Угрозы уязвимости информационной инфраструктуры критически важных объектов.
43. Негативные последствия нарушения функционирования систем управления критически важных объектов.
44. Определение требований к защите информации в АСУ ТП.
45. Разработка и внедрение защиты АСУ ТП.
46. Обеспечение защиты информации в ходе эксплуатации АСУ ТП.

**6.3. Типовые контрольные вопросы и задания для промежуточной аттестации**

Перечень вопросов к экзамену.
1. Понятие национальной безопасности. Основные угрозы и критерии оценки со-стояния национальной безопасности России.
2. Категории персональных данных. Уровни защищенности информационной сис-темы персональных данных (ИСПД).
3. Понятие информационной безопасности. Интересы личности, общества и госу-дарства в информационной сфере.
4. Обязанности обладателя конфиденциальной информации по ее защите.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
6. Требования к обеспечению безопасности ИСПД в зависимости от уровня защи-щенности ИСПД.
7. Угрозы информационной безопасности Российской Федерации.
8. Понятие информационной войны, цели и средства её ведения.
9. Контроль и надзор в сфере обеспечения информационной безопасности.
10. Понятие и основные свойства информации. Виды защищаемой информации.
11. Конституция РФ о правах и обязанностях граждан в информационной сфере.
12. Общие принципы и методы обеспечения информационной безопасности РФ.
13. Основные направления обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ). Порядок категорирования объектов КИИ.
14. Состав преступления, предусмотренный статьей 274 УК РФ.
15. Задачи единой государственной системы обнаружения и предупреждения компь-ютерных атак на критически важную информационную инфраструктуру (Гос-СОПКА)..
16. Должностные обязанности руководителя подразделения информационной безо-пасности.
17. Правовой режим защиты государственной тайны. Порядок допуска к сведениям, составляющим гостайну.

18. Состав и содержание организационных и технических мер по защите ИСПД.
19. Правовой режим защиты коммерческой тайны.
20. Процедура оценки обстановки на объекте защиты.
21. Состав преступления, предусмотренный статьей 272 УК РФ.
22. Типовые и частные модели угроз безопасности ИСПД.
23. Состав преступления, предусмотренный статьей 273 УК РФ.
24. Состав и содержание организационных и технических мер по защите значимого объекта КИИ.
25. Состав преступления, предусмотренный статьей 274.1 УК РФ.
26. Этапы создания и структура службы безопасности предприятия.
27. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
28. Задачи подразделения информационной безопасности предприятия.
29. Комплексная защита информации – сущность и задачи.
30. Должностные обязанности администратора безопасности АИС.
31. Компетенция ФСБ России в сфере обеспечения информационной безопасности.
32. Обязанности пользователя АИС по обеспечению информационной безопасности.
33. Понятие объекта КИИ. Порядок категорирования объектов КИИ.
34. Компетенция ФСТЭК России в сфере обеспечения информационной безопасно-сти.
35. Обязанности оператора по защите персональных данных.
36. Классификация информационного оружия.

### 6.4. Критерии оценивания

Допуском к экзамену является сделанный доклад на выбранную тему.
Экзамен проходит в виде теста в системе электронного обучения MOODLE.

Сводная таблица рейтинга успеваемости

| № | Перечень контрольных мероприятий в семестре | Максимальное кол-во баллов |
|---|---|---|
| 1 | Экзамен | 100 |
| Итого | | 100 |

При подведении итогов учитываются результаты текущей аттестации:
Отлично/зачтено/91-100 баллов
Хорошо/зачтено/75-90 баллов
Удовлетворительно/зачтено/61-74 балла
Неудовлетворительно/не зачтено/0-60 баллов.

## 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 | Рытенкова О. | Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=230502) | Москва : ГРОТЕК, 2014 | ЭБС |
| Л1.2 | Партыка Т. Л., Попов И.И. | Информационная безопасность: учебное пособие (https://znanium.com/catalog/document?id=364624) | Москва : Издательство "ФОРУМ", 2021 | ЭБС |
| Л1.3 | Мельников В.П., Куприянов А.И., Мельников В.П. | Информационная безопасность: учебник (https://book.ru/book/939292) | Москва : КноРус, 2021 | ЭБС |

#### 7.1.2. Дополнительная литература

| | Авторы, составители | Заглавие | Издательство, год | Ресурс |
|---|---|---|---|---|
| Л2.1 | Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н. | Организационно-правовое и методическое обеспечение информационной безопасности (https://e.lanbook.com/book/91449) | Санкт- Петербург : НИУ ИТМО, 2016 | ЭБС |
| Л2.2 | Загинайлов Ю. Н. | Основы информационной безопасности: курс визуальных лекций: учебное пособие (https://biblioclub.ru/index.php?page=book&id=362895) | Москва, Берлин : Директ-Медиа, 2015 | ЭБС |

| | Авторы, составители | Заглавие | Издательство, год | Ресурс |
|---|---|---|---|---|
| Л2.3 | | Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=458012) | Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016 | ЭБС |

**7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"**

| | |
|---|---|
| Э1 | Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru БД «Информационно-правовая система «Законодательство России» http://pravo.gov.ru/proxy/ips/?start_search&fattrib=1 |
| Э2 | Кодексы и законы РФ - правовая справочно-консультационная система http://kodeks.systecs.ru |

**7.3 Перечень информационных технологий**

**7.3.1 Программное обеспечение**

Adobe Reader

LMS Moodle

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 основные понятия, принципы, уровни и угрозы информационной безопасности. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических 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.

**Направление подготовки (специальность) 44.03.05 Педагогическое образование (с двумя профилями подготовки)**
**Направленность (профиль) Экономика и информатика**
**Рабочая программа дисциплины «Компьютерная безопасность»**
**2025 год набора, очная форма обучения**

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом факультета экономики и управления

Протокол заседания № 1 от 11.02.2025

Председатель Ученого совета факультета экономики и управления согласовано А. А. Егорова

**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**