Рабочая программа дисциплины (модуля)*

Программно-аппаратные средства защиты информации

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация N 4 "Безопасность автоматизированных систем критически важных объектов"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2026

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

Челябинск 2026 г.

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
6.1. Перечень видов оценочных средств
6.2. Типовые контрольные задания и иные материалы для текущей аттестации
6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
7.1. Рекомендуемая литература
7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины - формирование у студентов знаний по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств, а также навыков и умений по применению программно-аппаратных средств защиты информации в конкретных условиях.

Задачи дисциплины - дать знания:

- по концепции обеспечения информационной безопасности компьютерных систем;
- программно-аппаратным средствам, реализующим отдельные функциональные требования по защите;
- методам и средствам хранения ключевой информации;
- методам и средствам ограничения доступа к компонентам вычислительных систем;
- методам защиты от вредоносных программ;
- защите программ от изменения и контролю целостности;
- задачам и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности

Индикаторы достижения компетенций:

ОПК-2.1. Обладает знаниями о современных программных средствах системного и прикладного назначений, в том числе отечественного производства, в своей профессиональной области.

ОПК-2.2. Демонстрирует умения применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.25

2.1 Требования к предварительной подготовке обучающегося:

Языки программирования

Введение в специальность

Языки программирования (дополнительные главы)

Организация ЭВМ и вычислительных систем

Лаборатория аппаратных средств вычислительной техники

Электроника и схемотехника

Технологии и методы программирования

Лаборатория электроники и схемотехники

Сети и системы передачи информации

Безопасность сетей ЭВМ

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

Производственная практика (преддипломная практика)

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

ОПК-2: Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

Знать:

Для достижения индикатора ОПК-2.1: Знать о современных программных средствах системного и прикладного назначений, в том числе отечественного производства, в своей профессиональной области (SecretNet, БлокХост, Аккорд, Соболь, HASP, Guardian, Kaspersky, Dr.Web, Norton, Avast, Eset NOD).

Уметь:

Для достижения индикатора ОПК-2.2: Уметь применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

Владеть:

Для достижения индикатора ОПК-2.2: Владеть навыками применения программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
3.1.2	особенности применения программно-аппаратных средств обеспечения информационной безопасности;
3.1.3	типовые модели управления доступом;
3.1.4	типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
3.1.5	типовые средства и методы ведения аудита и обнаружения вторжений;
3.1.6	типовые средства и методы обеспечения информационной безопасности в сетях ЭВМ.
3.2	**Уметь:**
3.2.1	применять программно-аппаратные средства обеспечения информационной безопасности;
3.2.2	диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
3.2.3	оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
3.2.4	участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
3.2.5	применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
3.3	**Владеть:**
3.3.1	навыками применения программно-аппаратных средств обеспечения информационной безопасности;
3.3.2	навыками диагностики, устранения отказов и восстановление работоспособности программно- аппаратных средств обеспечения информационной безопасности;
3.3.3	навыками мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
3.3.4	навыками применения нормативно правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану: 144 в том числе: аудиторные занятия: 68 самостоятельная работа: 36,7 часов на контроль: 36 контактная работа: 71,3 ИКР: 3,3	Виды контроля в семестрах: экзамены 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.			
1.1	Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. Обеспечение гарантий выполнения политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды. /Лек/	7	10	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5

1.2	Разработка архитектуры системы защиты информации автоматизированной системы с применением программно- аппаратных средств защиты информации. Построение моделей защищенной автоматизированной системы. Изучение методов идентификации и аутентификации с применением программно-аппаратных средств защиты информации. /Лаб/	7	10	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
1.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 2. Программно-аппаратные средства обеспечения информационной безопасности			
2.1	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно- аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности. /Лек/	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
2.2	Изучение современных программно-аппаратных средств обеспечения информационной безопасности. Назначение, функции, область применения программно-аппаратных средств защиты информации. Изучение и сравнение особенностей и аналогов программно- аппаратных средств обеспечения информационной безопасности различных категорий. Освоение новых образцов программных средств. Контрольные проверки работоспособности применяемых программно-аппаратных средств защиты информации. /Лаб/	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
2.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации			
3.1	Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий /Лек/	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
3.2	Изучение нормативной документации, в том числе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации.	7	12	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
3.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	7	12,7	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Иная контактная работа			
4.1	Индивидуальные консультации, текущий контроль /ИКР/	7	3,3	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по лабораторным работам.
Реферат
Тест
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Собеседование по темам лабораторных занятий:
1) Разработка архитектуры системы защиты информации автоматизированной системы с применением программно-аппаратных средств защиты информации.
2) Построение моделей защищенной автоматизированной системы.
3) Изучение методов идентификации и аутентификации с применением программно-аппаратных средств защиты информации.
4) Изучение современных программно-аппаратных средств обеспечения информационной безопасности.
5) Назначение, функции, область применения программно-аппаратных средств защиты информации.
6) Изучение и сравнение особенностей и аналогов программно-аппаратных средств обеспечения информационной безопасности различных категорий.
7) Освоение новых образцов программных средств.
8) Контрольные проверки работоспособности применяемых программно-аппаратных средств защиты информации.
9) Изучение нормативной документации, в том числе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации.
10) Поиск программно-аппаратных средств защиты информации, соответствующих требованиям руководящих документов.

Примерная тематика рефератов:
1) Дискреционная модель доступа к файлам;
2) Мандатное управление доступом;
3) Проверка целостности файлов;
4) Программа для аутентификации с помощью usb-устройства;
5) Аутентификация с использованием ключа eToken;
6) Разграничение доступа к принтерам;
7) Разграничение доступа к устройствам. Флеш-накопители;
8) Реализация асимметричного шифрования;
9) Реализация симметричного шифрования;
10) Расширение базовой системы аутентификации Windows;
11) Антифишинговый фильтр;
12) Программный межсетевой экран;
13) Разработка защиты от программ слежения за набором на клавиатуре

Типовой тест:
1. На что направлены программно-технические меры:
А) На контроль оборудования
Б) На контроль программ
В) На контроль данных
Г) На контроль компьютерных сущностей
2. Почему бурное развитие информационных технологий объективно затрудняет обеспечение надежной защиты:
А) Конкуренция среди производителей программного обеспечения приводит к повышению качества тестирования
Б) Развитие архитектур и микросхем позволяет преодолевать барьеры ранее казавшиеся недоступными
В) Появление новых информационных сервисов ведет к образованию новых уязвимых мест
Г) Развитие сетей сужает круг злоумышленников, имеющих техническую возможность организовать атаки
3. Что относится к вспомогательным сервисам безопасности:
А) Экранирование
Б) Сервисы безопасности
В) Шифрование
Г) Управление
4. Какие виды мер безопасности существуют:
А) Локализующие
Б) Превентивные
В) Восстановления режима безопасности
Г) Прогнозирующие

5. К каким мерам безопасности относится обеспечение отказоустойчивости:
А) Превентивные
Б) Обнаружения нарушений
В) Локализующие
Г) По выявлению нарушителя
6. Какие принципы вытекают из теоретической основы решения проблемы архитектурной безопасности:
А) Необходимость выработки единой политики безопасности
Б) Необходимость обеспечения целостности при сетевых взаимодействиях
В) Не должно быть информационных потоков, идущих к незащищенным сервисам
Г) Необходимость формирования составных сервисов по содержательному принципу
7. Что относится к принципам архитектурной безопасности:
А) Усиление самого слабого звена
Б) Невозможность миновать защитные средства
В) Разнообразие защитных средств
Г) Управляемость информационной системы
8. Иерархическая организация информационной системы необходима для:
А) Повышения надежности информационной системы
Б) Уменьшения ущерба от случайных действий пользователей
В) Обеспечения управляемости системой
Г) Технологических соображений
9. Какие принципы необходимо соблюдать для обеспечения непрерывности функционирования информационной системы:
А) Минимизация объема защитных средств
Б) Внесение в конфигурацию формы избыточности
В) Наличие единой точки отказа
Г) Выделение подсетей и изоляция групп пользователей друг от друга
10. Причины использования минимизации объема защитных средств:
А) Рассредоточенность сетевого управления
Б) Конфигурации клиентских систем трудно или невозможно контролировать
В) Для доступа в корпоративную сеть могут использоваться потребительские устройства с ограниченной функциональностью
Г) Наличие средств обнаружения нештатных ситуаций

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену:
1) Понятие политики безопасности. Описание типовых политик безопасности.
2) Угрозы безопасности компьютерных систем. Модель компьютерной системы.
3) Понятие монитора безопасности. Концепция диспетчера доступа.
4) Обеспечение гарантий выполнения политики безопасности.
5) Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.
6) Модели безопасного взаимодействия в КС.
7) Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.
8) Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.
9) Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности.
11) Взаимодействие с общесистемными компонентами вычислительных систем.
12) Методы и средства ограничения доступа к компонентам вычислительных систем.
13) Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
14) Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
15) Защита программ от изучения.
16) Способы встраивания средств защиты в программное обеспечение.
17) Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
18) Защита программ от изменения и контроль целостности.
19) Роль стандартов информационной безопасности. Документы Государственной технической комиссии России.
20) Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
21) Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.

22) Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем.
23) Требования к процессу сертификации продукта информационных технологий

6.4. Критерии оценивания

Критерии оценивания собеседования и отчета по лабораторным работам:
В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.
Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет, владеет методикой обработки экспериментальных данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.
Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Критерии оценивания реферата:
Реферат – творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования. Цель написания реферата – привитие студенту навыков краткого и лаконичного представления собранных материалов и фактов в соответствии с требованиями, предъявляемыми к научным отчетам, обзорам и статьям. Реферат оценивается руководителем исходя из установленных показателей и критериев оценки реферата:
1) Новизна реферированного текста (Макс. - 5 баллов)
- актуальность проблемы и темы;
- новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы;
- наличие авторской позиции, самостоятельность суждений.
2) Степень раскрытия сущности проблемы (Макс. - 5 баллов)
- соответствие плана теме реферата;
- соответствие содержания теме и плану реферата;
- полнота и глубина раскрытия основных понятий проблемы;
- обоснованность способов и методов работы с материалом;
- умение работать с литературой, систематизировать и структурировать материал;
- умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
3) Обоснованность выбора источников (Макс. - 5 баллов)
- круг, полнота использования литературных источников по проблеме;
- привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).
4) Соблюдение требований к оформлению (Макс. - 5 баллов)
- правильное оформление ссылок на используемую литературу;
- грамотность и культура изложения;
- владение терминологией и понятийным аппаратом проблемы;
- соблюдение требований к объему реферата;
- культура оформления: выделение абзацев.
5) Грамотность (Макс. - 5 баллов)
- отсутствие орфографических и синтаксических ошибок, сти-листических погрешностей;
- отсутствие опечаток, сокращений слов, кроме общепринятых;
- литературный стиль
Реферат оценивается по 25 балльной шкале, балы переводятся в оценки успеваемости следующим образом:
15 баллов и выше - "зачтено"
меньше 15 баллов - "незачтено"

Критерии оценивания теста:
Тест - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Важнейшими достоинствами тестов являются:
1) экономия времени преподавателя
2) возможность поставить всех студентов в одинаковые условия
3) возможность разработки равноценных по трудности вариантов вопросов
4) возможность проверить обоснованность оценки
5) уменьшение субъективного подхода к оценке подготовки студента, обусловленного его индивидуальными особенностями
За тест ставится оценка "зачтено", если выполнено правильно более половины заданий.

Критерии оценивания экзамена:
Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.
Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается. Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».
Оценка «отлично» выставляется:
Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.
Оценка «хорошо» выставляется:
Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.
Оценка «удовлетворительно» выставляется:
Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.
Оценка «неудовлетворительно» выставляется:
1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.
2) Ответ на вопрос полностью отсутствует.
3) Отказ от ответа.

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	Душкин А.В., Кольцов А.С., Кравченко А.С., Ланкин О.В.	Аппаратные и программные средства защиты информации: учебное пособие (https://znanium.com/catalog/document?id=242398)	Воронеж : Издательско-полиграфический центр "Научная книга", 2016	ЭБС
Л1.2	Хорев П. Б.	Программно-аппаратная защита информации: учебное пособие (https://znanium.com/catalog/document?id=397282)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2022	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов (https://urait.ru/bcode/562070)	Москва : Юрайт, 2025	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. - URL: https://urait.ru/
Э4	Znanium.com [Электронный ресурс] : электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. – URL: http://znanium.com/
Э5	eLIBRARY.RU [Электронный ресурс] : электронная библиотека / Науч. электрон. б-ка. – URL: http://elibrary.ru/defaultx.asp

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

OpenOffice

Adobe Reader

WinDjView

LMS Moodle

Adobe Connect Acrobat

ПО Kaspersky

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. APS JOURNALS. Physical Review Letters, Physical Review X, Physical Review, and Reviews of Modern Physics : журналы American Physical Society : сайт. – URL: http://journals.aps.org/about – Яз. англ. – Режим доступа: только из сети университета. – Текст : электронный.

3. Web of Science : мультидисциплинарная реферативная база данных / компания Thomson Reuters. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

4. Scopus : реферативная база данных / Elsevier BV. – URL: http://www.scopus.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

5. Springer Link : [сайт]. – URL: http://link.springer.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения - мультимедийным оборудованием (экран, ноутбук, проектор, колонки).

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно- наглядных пособий (мультимедийные презентации), различные формы наглядности (графики, таблицы, схемы и т.д)).

Лабораторные занятия проходят в учебной лаборатории электроники и схемотехники, микропроцессорных систем (аудитория 221 учебный корпус №1). Материально - техническое обеспечение приведено в паспорте лаборатории.

Для самостоятельной работы студента используются аудитория №205 - читальный зал №3 (учебный корпус №1) и аудитория №206 - электронный читальный зал (специализированный медиацентр) (учебный корпус №1), оснащенные персональными компьютерами, мультимедийной аппаратурой. В аудиториях обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

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

Освоение содержания учебной дисциплины «Программно-аппаратные средства защиты информации» осуществляется на лекциях, лабораторных занятиях и в процессе самостоятельной учебной деятельности студентов.

Лекции составляют основу теоретической подготовки студентов с целью понимания ими сущности дисциплины. Лекционные занятия посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку. В ходе лекционных занятий нужно конспектировать учебный материал, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений. Лекции должны активизировать познавательную деятельность обучающихся, вызывать интерес к поставленным проблемам и направлениям развития в профессиональной области, формировать их профессиональный кругозор, аналитические качества, творческий подход к изучению дисциплины, определять направления дальнейшего самостоятельного изучения и практического освоения в данной области. Изложение материала лекций должно носить проблемный, инновационный характер, способствующий формированию и развитию соответствующих компетенций. Преподавателю необходимо опираться на основную литературу, представленную в рабочей программе данной дисциплины, а также на учебные пособия, монографии, научные статьи и периодические издания известных специалистов в данной области.

Лабораторные занятия предназначены для приобретения опыта практической реализации полученных теоретических знаний. Указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется преподавателем перед проведением лабораторных занятий. На лабораторных занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения производственной практики.

Самостоятельная работа студентов включает проработку лекционного курса, подготовку к практическим работам, выполнение всех заявленных в рабочей программе видов самостоятельной работы (выполнение домашних заданий). Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников. В ходе самостоятельной работы необходимо изучить основную литературу, ознакомиться с дополнительной литературой. Очень полезно дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.

Рекомендации по написанию реферата:

1) Тема реферата выбирается в соответствии с интересами студента и не обязательно должна соответствовать приведенному примерному перечню. Важно, чтобы в реферате были освящены стороны проблемы, а также представлены теоретические положения и конкретные примеры.

2) Реферат должен основываться на проработке нескольких дополнительных к основной литературе источников. Как правило это научные монографии или статьи.

3) План реферата должен быть авторским. В нем проявляется подход автора, его мнение, анализ проблемы.

4) Все приводимые в реферате факты и заимствованные соображения должны сопровождаться ссылками на источник информации.

5) Недопустимо просто скомпоновать реферат из кусков заимствованного текста. Все цитаты должны быть представлены в кавычках с указанием в скобках источника и страницы.

6) Реферат оформляется в виде текста на листах формата А-4. Работа начинается с титульного листа, в котором указывается название университета, название кафедры, учебной дисциплины, тема реферата, ФИО студента, номер группы, год и географическое место местонахождения университета. Затем следует оглавление с указанием страниц разделов. Сам текст реферата желательно подразделить на разделы: главы, подглавы и озаглавить их. Приветствуется использование в реферате количественных данных и иллюстраций (графики, таблицы, диаграммы, рисунки).

7) Завершают реферат разделы «Заключение» и «Список использованной литературы». В заключении должны быть представлены основные выводы, ясно сформулированные в тезисной форме.

8) Источник литературы должен быть составлен в полном соответствии с действующим стандартом (правилами), включая особую расстановку знаков препинания.

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, MS Office365, форумы, электронная почта и др.).

При обучении инвалидов и 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.

Рабочая программа дисциплины (модуля) одобрена и рекомендована:
Проректор по учебной работе утверждено 27.02.26 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 04 от 05.02.2026

Председатель Ученого совета
физического факультета согласовано М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 03.02.2026

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) М.Е. Беленков

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13»апреля 2021 г. № 274-1