Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таскаев Сергей Валерьевич
Должность: Ректор
Дата подписания: 04.04.2025 17:45:57
Уникальный программный ключ:
04c19ed8bfb98f5b6cb77a486b9a878db8322323

УТВЕРЖДАЮ
Проректор по учебной работе
_____ / В.Е. Федоров
«23» июня 2021 г.

Рабочая программа дисциплины (модуля)*

Инновационные методы 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 2021

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

Челябинск 2021 г.

© ФГБОУ ВО «ЧелГУ»

Рабочая программа дисциплины (модуля) принята:

Ученым советом физического факультета

Протокол заседания № 11 от «27» мая 2021 г.

Председатель Ученого совета физического факультета _____ Д.А. Захарьевич

Секретарь Ученого совета физического факультета _____ М.А. Эбель

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой

Радиофизики и электроники

Протокол заседания № 10 от «24» мая 2021 г.

И.о зав. кафедрой _____ А.В. Бутаков

Автор (составитель) _____ к.ф.-м.н., доцент кафедры радиофизики и электроники А.В. Бутаков

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

© ФГБОУ ВО «ЧелГУ»

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

© ФГБОУ ВО «ЧелГУ»

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины - выработка навыков по формированию системного подхода к проблеме анализа и синтеза средств защиты информации, основываясь на инновационных методах защиты информации.

Задачи дисциплины:

1. Умение квалифицированно и оперативно оценить надежность применяемой в данной ситуации системы информационной безопасности.

2. Умение квалифицированно и оперативно выбирать или синтезировать системы информационной информации (СИБ), адекватно регулирующие на возможные в данной ситуации виды умышленных угроз для безопасности информации.

3. Умение квалифицированно и оперативно выбирать или синтезировать нужные в данной конкретной ситуации по обеспечению информационной безопасности технические средства защиты.

4. Умение квалифицированно и оперативно оценить надежность применяемой в данной ситуации системы информационной безопасности.

Индикаторы достижения компетенций:

ПК-2.1. Обладает знаниями моделирования и исследования систем защиты информации автоматизированных систем.

ПК-2.2. Демонстрирует умение разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, и применять эти модели при проектировании систем защиты информации автоматизированных систем.

ПК-2.3. Имеет практический опыт (навыки) оценки защищенности информации в автоматизированных системах и выбора обоснованных решений по обеспечению эффективности средств и способов их защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.ДВ.01.02

2.1 Требования к предварительной подготовке обучающегося:

Информатика

Языки программирования

Введение в специальность

Языки программирования (дополнительные главы)

Физика

Алгебра

Математический анализ

Системное программное обеспечение и аппаратное программирование

Организация ЭВМ и вычислительных систем

Основы радиотехники

Лаборатория аппаратных средств вычислительной техники

Электроника и схемотехника

Теория информации

Сети и системы передачи информации

Лаборатория электроники и схемотехники

Криптографические протоколы

Безопасность сетей ЭВМ

Безопасность операционных систем

Программно-аппаратные средства защиты информации

Техническая защита информации

Инженерно-техническая защита информации и технические средства охраны на критически важных объектах

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

© ФГБОУ ВО «ЧелГУ»

Научно-исследовательская работа

Защита информации от утечки по техническим каналам

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)

ПК-2: Способен создавать и исследовать модели автоматизированных систем, проводить анализ их защищенности, а также предлагать и обосновывать выбор решений по обеспечению эффективности средств и способов защиты информации;

Знать:

Для достижения индикатора ПК-2.1: Знать моделирование и исследование систем защиты информации автоматизированных систем (инновационные методы защиты информации, модели данных, систем и процессов защиты информации в автоматизированных системах, критерии оценки защищенности автоматизированных систем, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, методы и модели анализа угроз безопасности подсистем автоматизированных систем).

Уметь:

Для достижения индикатора ПК-2.2: Уметь разрабатывать и исследовать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, и применять эти модели при проектировании систем защиты информации автоматизированных систем (оценить надежность применяемой в данной ситуации системы информационной безопасности, выбирать или синтезировать системы информационной информации (СИБ), адекватно регулирующие на возможные в данной ситуации виды умышленных угроз для безопасности информации, выбирать или синтезировать нужные в данной конкретной ситуации по обеспечению информационной безопасности технические средства защиты, оценить надежность применяемой в данной ситуации системы информационной безопасности, выявлять уязвимости информационно-технологических ресурсов автоматизированных систем).

Владеть:

Для достижения индикатора ПК-2.3: Владеть навыками оценки защищенности информации в автоматизированных системах и выбора обоснованных решений по обеспечению эффективности средств и способов их защиты (методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем).

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	инновационные методы защиты информации;
3.1.2	модели данных, систем и процессов защиты информации в автоматизированных системах;
3.1.3	критерии оценки защищенности автоматизированных систем;
3.1.4	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
3.1.5	методы и модели анализа угроз безопасности подсистем автоматизированных систем
3.2	**Уметь:**
3.2.1	оценить надежность применяемой в данной ситуации системы информационной безопасности;
3.2.2	выбирать или синтезировать системы информационной информации (СИБ), адекватно регулирующие на возможные в данной ситуации виды умышленных угроз для безопасности информации;
3.2.3	выбирать или синтезировать нужные в данной конкретной ситуации по обеспечению информационной безопасности технические средства защиты;
3.2.4	оценить надежность применяемой в данной ситуации системы информационной безопасности;
3.2.5	выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
3.3	**Владеть:**
3.3.1	методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**5 ЗЕТ**
Часов по учебному плану: 180 в том числе: аудиторные занятия: 72 самостоятельная работа: 90 часов на контроль: 18	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. Инновационные методы защиты информации			

© ФГБОУ ВО «ЧелГУ»

1.1	Основные понятия теории защиты информации в измерительных системах и информационных технологиях управления объектом. Виды умышленных угроз безопасности информации. Методы и технические средства построения технических систем информационной безопасности, их структура. Криптографические методы защиты информации. Анализ и особенности каналов утечки и несанкционированного доступа к информации в технических информационных системах. Аппаратная реализация современных технических методов несанкционированного доступа к информации. Современные технические средства обнаружения угроз. Современные технические средства обеспечения безопасности к каналах информационно-вычислительных систем, телекоммуникаций и ЭВМ. Современные технологические средства защиты информации от несанкционированного доступа в сетях ЭВМ. Основнык понятия моделирования больших систем. Математическое моделирование больших систем на основе математических систем: A-схем, D-схем, F-схем, P-схем, Q-схем. Основные понятия теории надежности систем. Метод расчета надежности систем на базе построения логической функции системы. Метод расчета вероятности взлома системы на основе логической функции системы. Концепция интегральной защиты информации. Компютерная стенография как перспективное, современное, техническое и программное средство защиты информации, от несанкционированного доступа. Технические средства и технологии, информационных систем безопасности от электромагнитного терроризма. Вредоносные вирусные программы. Современные технические средства борьбы с компьютерными вирусами. Содержание метода временных диаграмм, его графическое представление. Исследование причин универсальности этого метода в задачах моделирования работы сложенных многоканальных систем управления безопасностью объектов. /Лек/	9	36	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2 Э3 Э4 Э5
1.2	Анализ основных технических средств для несанкционированного добывания информации. Сравнительные характеристики пассивных средств получения информации. Сравнительные характеристики активных средств получения информации. Изучение основных положений концепции безопасности автоматизированных систем обработки информации. Симметрические криптосистемы: подстановки, перестановки, гаммирование, блочные шифры. Системы с открытым ключом. Алгоритм RSA. Сравнительные технические характеристики пассивных и активных средств незаконного получения информации. Методы защиты. Современные угрозы информации в информационно- вычислительных системах и телекоммуникационных каналах связи. Основы концепции интегральной безопасности объекта. Сравнительный анализ технических характеристик сканеров и нелинейных радиолокаторов при их применении для решения задач обнаружения радиопередатчиков в ближней зоне этих передатчиков. Анализ факторов, существенно влияющих на безопасность распределенных систем и анализ угроз для сетей ЭВМ. Разработка моделирующего алгоритма для системы безопасности, представленный в виде многоканальной Q-схемы. Процедура формализации систем («охраняемых объектов») с использованием A-схемы. Построение моделирующих алгоритмов. Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого D- схемой.	9	36	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2 Э3 Э4 Э5

© ФГБОУ ВО «ЧелГУ»

	Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого F- схемой. Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого P- схемой. Основы логических расчетов надежности автоматизированных систем безопасности. Структурная схема объекта (системы). Принципы составления логической функции работоспособности объекта (системы). Приведение логической функции работоспособности системы безопасности к элементарному виду. Алгоритм расчета вероятности взлома системы безопасности, основанный на логической функции работоспособности системы. Методы приведения логической функции системы безопасности к элементарному виду для задачи несанкционированного доступа в систему безопасности. Основные каналы силового деструктивного воздействия; технические средства, реализующие и защищающие от электромагнитного терроризма. /Лаб/			
1.3	Проработка лекционного материала и подготовка к лабораторным работам. /Ср/	9	90	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по лабораторным работам
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Собеседование по темам лабораторных занятий:

1. Анализ основных технических средств для несанкционированного добывания информации.
2. Сравнительные характеристики пассивных средств получения информации.
3. Сравнительные характеристики активных средств получения информации.
4. Изучение основных положений концепции безопасности автоматизированных систем обработки информации.
5. Симметрические криптосистемы: подстановки, перестановки, гаммирование, блочные шифры. Системы с открытым ключом. Алгоритм RSA.
6. Сравнительные технические характеристики пассивных и активных средств незаконного получения информации. Методы защиты.
7. Современные угрозы информации в информационно-вычислительных системах и телекоммуникационных каналах связи.
8. Основы концепции интегральной безопасности объекта.
9. Сравнительный анализ технических характеристик сканеров и нелинейных радиолокаторов при их применении для решения задач обнаружения радиопередатчиков в ближней зоне этих передатчиков.
10. Анализ факторов, существенно влияющих на безопасность распределенных систем и анализ угроз для сетей ЭВМ.
11. Разработка моделирующего алгоритма для системы безопасности, представленный в виде многоканальной Q- схемы.
12. Процедура формализации систем («охраняемых объектов») с использованием A-схемы. Построение моделирующих алгоритмов.
13. Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого D-схемой.
14. Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого F-схемой.
15. Разработка алгоритма, моделирующего процесс функционирования системы безопасности объекта, представляемого P-схемой.
16. Основы логических расчетов надежности автоматизированных систем безопасности. Структурная схема объекта (системы). Принципы составления логической функции работоспособности объекта (системы).
17. Приведение логической функции работоспособности системы безопасности к элементарному виду.
18. Алгоритм расчета вероятности взлома системы безопасности, основанный на логической функции работоспособности системы.
19. Методы приведения логической функции системы безопасности к элементарному виду для задачи несанкционированного доступа в систему безопасности.
20. Основные каналы силового деструктивного воздействия; технические средства, реализующие и защищающие от

© ФГБОУ ВО «ЧелГУ»

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену:
1. Основные понятия теории защиты информации в измерительных системах и информационных технологиях управления объектом.
2. Виды умышленных угроз безопасности информации.
3. Методы и технические средства построения технических систем информационной безопасности, их структура.
4. Криптографические методы защиты информации.
5. Анализ и особенности каналов утечки и несанкционированного доступа к информации в технических информационных системах.
6. Аппаратная реализация современных технических методов несанкционированного доступа к информации.
7. Современные технические средства обнаружения угроз.
8. Современные технические средства обеспечения безопасности к каналах информационно-вычислительных систем, телекоммуникаций и ЭВМ.
9. Современные технологические средства защиты информации от несанкционированного доступа в сетях ЭВМ.
10. Основнык понятия моделирования больших систем. Математическое моделирование больших систем на основе математических систем: A-схем, D-схем, F-схем, P-схем, Q-схем.
11. Основные понятия теории надежности систем. Метод расчета надежности систем на базе построения логической функции системы.
12. Метод расчета вероятности взлома системы на основе логической функции системы.
13. Концепция интегральной защиты информации.
14. Компютерная стенография как перспективное, современное, техническое и программное средство защиты информации, от несанкционированного доступа.
15. Технические средства и технологии, информационных систем безопасности от электромагнитного терроризма.
16. Вредоносные вирусные программы. Современные технические средства борьбы с компьютерными вирусами.
17. Содержание метода временных диаграмм, его графическое представление. Исследование причин универсальности этого метода в задачах моделирования работы сложенных многоканальных систем управления безопасностью объектов.

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 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.

© ФГБОУ ВО «ЧелГУ»

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	Куняев Н. Н.	Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: монография (https://biblioclub.ru/index.php?page=book&id=84990)	Москва : Логос, 2010	ЭБС
Л1.2	Кузовкин В. А.	Электроника. Электрофизические основы, микросхемотехника, приборы и устройства: учебник (https://biblioclub.ru/index.php?page=book&id=89796)	Москва : Логос, 2011	ЭБС
Л1.3	Башлы П. Н., Баранова Е. К., Бабаш А. В.	Информационная безопасность: учебно-практическое пособие: учебное пособие (https://biblioclub.ru/index.php?page=book&id=90539)	Москва : Евразийский открытый институт, 2011	ЭБС
Л1.4	Круг К. А.	Физические основы электротехники (https://biblioclub.ru/index.php?page=book&id=213666)	Москва, Ленинград : Государственное энергетическое издательство, 1946	ЭБС
Л1.5	Гатчин Ю. А., Сухостат В. В., Куракин А. С., Донецкая Ю. В.	Теория информационной безопасности и методология защиты информации: учебное пособие (https://e.lanbook.com/book/136476)	Санкт- Петербург : НИУ ИТМО, 2018	ЭБС
Л1.6	Ярочкин В.И.	Информационная безопасность: учебник (https://www.studentlibrary.ru/book/ISBN9785829130312.html)	Москва : Академический Проект, 2020	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Фомин С. А.	Обеспечение национальной безопасности: курс лекций (https://e.lanbook.com/book/122707)	Москва : ФЛИНТА, 2019	ЭБС
Л2.2	Суворова Г. М.	Информационная безопасность: учебное пособие для вузов (https://urait.ru/bcode/467370)	Москва : Юрайт, 2021	ЭБС
Л2.3	Внуков А. А.	Защита информации: учебное пособие для вузов (https://urait.ru/bcode/470131)	Москва : Юрайт, 2021	ЭБС
Л2.4	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов (https://urait.ru/bcode/469866)	Москва : Юрайт, 2021	ЭБС
Л2.5	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов (https://urait.ru/bcode/477968)	Москва : Юрайт, 2021	ЭБС

© ФГБОУ ВО «ЧелГУ»

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

Adobe Connect Acrobat

LMS Moodle

MS Office365

Adobe Reader

WinDjView

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) и в учебной лаборатории технических средств защиты информации автоматизированных систем (аудитория 215 лабораторный корпус). Материально - техническое обеспечение приведено в паспорте лабораторий.

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 «Инновационные методы 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

© ФГБОУ ВО «ЧелГУ»

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, подготовка к тестам). 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.
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 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 голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.
1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся 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 к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:

© ФГБОУ ВО «ЧелГУ»

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления 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 технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. 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.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

© ФГБОУ ВО «ЧелГУ»