

Документ подписан простой электронной подписью Информация о владельце: ФИО: Таскаев Сергей Валерьевич Должность: Ректор Дата подписания: 07.07.2024 16:04:19 Уникальный программный ключ: 891954b8c2cf7b6350abe51cddb3096c877fa167	МИНОВНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	Рабочая программа дисциплины "Защита информации от утечки по техническим каналам" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализации N1 "Анализ безопасности компьютерных систем" ФГБОУ ВО «ЧелГУ»	стр. 1
--	--	---	--------

Рабочая программа дисциплины (модуля)*
Защита информации от утечки по техническим каналам

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2024

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

Челябинск 2024 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

Целью освоения дисциплины «Защита информации от утечки по техническим каналам» является формирование у студентов целостного представления о принципах защиты информации техническими средствами; средствах выявления технических каналов утечки информации; технических средствах защиты объектов. Изучение теоретических основ и физической природы возникновения информационных сигналов в электромагнитных, электрических, акустических и виброакустических каналах утечки информации, методов расчета параметров, приобретение студентами навыков практической работы с техническими средствами защиты, а также контроля эффективности мер защиты информации и аттестации объектов информатизации.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем.

ОПК-6.2. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

ОПК-9.1. Знает технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации.

ОПК-9.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации.

ОПК-9.3. Владеет методами и средствами технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.28

2.1 Требования к предварительной подготовке обучающегося:

Физика

Аппаратные средства вычислительной техники

Электроника и схемотехника

Сети и системы передачи информации

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

Организационное и правовое обеспечение информационной безопасности

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

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

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Знать:



Для достижения индикатора ОПК-6.1: Знать систему нормативных правовых актов и стандартов по лицензированию в области технической защиты конфиденциальной информации; основные угрозы безопасности информации и модели нарушителя компьютерных систем

Уметь:

Для достижения индикатора ОПК-6.2: Уметь разрабатывать модели угроз и модели нарушителя компьютерных систем; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

Владеть:

Для достижения индикатора ОПК-6.2: Владеть навыками защиты информации от утечки по техническим каналам

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

Знать:

Для достижения индикатора ОПК-9.1: Знать технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; основные телекоммуникационные протоколы.

Уметь:

Для достижения индикатора ОПК-9.2: Уметь пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.

Владеть:

Для достижения индикатора ОПК-9.3: Владеть навыками решения задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Нормативно-правовую базу в области технической защиты информации. Физические основы функционирования технических средств, возникновения каналов утечки информационных сигналов, законы распространения сигналов различной природы в физических средах. Основные подходы к комплексному и целостному обеспечению информационной безопасности при помощи технических средств защиты.
3.2	Уметь:
3.2.1	Выявлять каналы утечки информации от технических средств, оценивать их актуальность и вероятность утечки информации. Проводить расчёт характеристик электромагнитных, звуковых полей и различных сигналов в линиях. Обеспечивать защиту от утечки информации по техническим каналам, защиту от НСД.
3.3	Владеть:
3.3.1	Навыками разработки и организации защиты от утечки информации по техническим каналам, защиты от НСД.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	4 ЗЕТ
Часов по учебному плану: 144 в том числе: аудиторные занятия: 68 самостоятельная работа: 38 часов на контроль: 27 контактная работа: 79 ИКР: 11	Виды контроля в семестрах: экзамены 8



5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Организационные основы инженерно-технической защиты информации			
1.1	Организационные основы инженерно-технической защиты информации. /Лек/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
1.2	Проработка лекционного материала. Государственная система защиты информации. /Ср/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 2. Концепции инженерно-технической защиты информации			
2.1	Основные свойства информации как предмета защиты. Концепции инженерно-технической защиты информации. /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
2.2	Проработка лекционного материала. Стандарты в области защиты информации. /Ср/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 3. Теоретические основы инженерно-технической защиты информации			
3.1	Теоретические основы инженерно-технической защиты информации. /Лек/	8	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 4. Физические основы защиты информации			
4.1	Физические основы защиты информации. /Лек/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 5. Технические средства защиты информации			
5.1	Технические средства защиты информации. /Лек/	8	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
5.2	Обнаружение и локализация источников радиоизлучений. Оценка защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН), анализатор спектра. Защита информации по каналам ПЭМИН. Оценка защищённости помещений от утечки информации по виброакустическому и акустическому каналам, защита акустической информации. Проверка на наличие технических средств негласного получения информации в помещении. Защита от НСД. /Лаб/	8	34	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
5.3	Проработка лекционного материала. Подготовка и оформление отчетов по лабораторным работам. /Ср/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 6. Методическое обеспечение инженерно-технической защиты автоматизированных систем			
6.1	Методическое обеспечение инженерно-технической защиты автоматизированных систем. /Лек/	8	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
6.2	Проработка лекционного материала. Методические рекомендации по оценке эффективности защиты информации. /Ср/	8	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1
	Раздел 7. Иная контактная работа			
7.1	Контактные часы на аттестацию Индивидуальные консультации, текущий контроль /ИКР/	8	11	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1



6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по лабораторным работам.
Вопросы к экзамену

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Типовые вопросы для собеседования по лабораторным работам:
Основные проблемы инженерно-технической защиты информации.
Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля.
Направления инженерно-технической защиты информации.
Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.
Информация как предмет защиты.
Аттестация объектов информатизации.
Демаскирующие признаки.
Акустический и виброакустический каналы утечки информации.
Виды побочных опасных электромагнитных излучений.
Основные физические характеристики акустических волн и восприятие их человеком.
Технические каналы утечки информации.
Технические средства негласного съема информации, применяемые в радиоэлектронном диапазоне длин волн.
Методы инженерной защиты и технической охраны объекта.
Построение каналов утечки информации в радиоэлектронном диапазоне длин волн.
Методы скрытия информации и ее носителей.
Органы добывания информации, структура органов разведки и ее виды. разведки коммерческих структур.
Распространение сигналов в технических каналах утечки информации.
Виды угроз безопасности информации, принципы добывания и обработки информации.
Средства технической разведки.
Побочные излучения и наводки.
Государственная система защиты информации.
Источники функциональных сигналов. Фильтрация информационных сигналов.
Контроль эффективности инженерно-технической защиты информации.
Источники опасных сигналов (физические поля, электрические сигналы).
Методические рекомендации по оценке эффективности защиты информации.
Нормативные документы по противодействию технической разведке.
Моделирование инженерно-технической защиты информации.
Способы записи информации на различные виды носителей и принципы съема информации.
Средства предотвращения утечки информации по техническим каналам. Пространственное и линейное зашумление.
Основные демаскирующие признаки радиолокационных станций, лазерных излучений.
Средства инженерной защиты и технической охраны. Система охранно-тревожной сигнализации. Система контроля и управления доступом.
Особенности видовых признаков в видимом, инфракрасном и радиодиапазонах электромагнитных волн.
Физические основы побочных электромагнитных излучений и наводок.
Классификация сигналов по форме, физической природе, виду информации и регулярности появления. Параметры сигналов.
Физические процессы подавления опасных сигналов.
Демаскирующие признаки веществ.
Методы инженерно-технической защиты информации.
Видовые, сигнальные и вещественные демаскирующие признаки. информационность признаков.
Каналы утечки информации за счет паразитных связей.
Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.
Характеристика технической разведки.
Объект защиты, носитель информации, информационные процессы.
Показатели эффективности инженерно – технической защиты информации.
Организационно – технические мероприятия по защите информации
Свойства информации, влияющие на ее безопасность.
Виды защищаемой информации. защита информации от утечки, непреднамеренного и несанкционированного воздействия на нее.
Системный подход к защите информации.
Ценность информации.
Основные концептуальные положения инженерно-технической защиты информации.
Основные свойства информации как предмета защиты.
Технические средства защиты информации. Средства выявления каналов утечки информации.



6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену:

1. Основные проблемы инженерно-технической защиты информации.
2. Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля.
3. Направления инженерно-технической защиты информации.
4. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.
5. Информация как предмет защиты.
6. Аттестация объектов информатизации.
7. Демаскирующие признаки.
8. Акустический и виброакустический каналы утечки информации.
9. Виды побочных опасных электромагнитных излучений.
10. Основные физические характеристики акустических волн и восприятие их человеком.
11. Технические каналы утечки информации.
12. Технические средства негласного съема информации, применяемые в радиоэлектронном диапазоне длин волн.
13. Методы инженерной защиты и технической охраны объекта.
14. Построение каналов утечки информации в радиоэлектронном диапазоне длин волн.
15. Методы скрытия информации и ее носителей.
16. Органы добывания информации, структура органов разведки и ее виды. разведки коммерческих структур.
17. Распространение сигналов в технических каналах утечки информации.
18. Виды угроз безопасности информации, принципы добывания и обработки информации.
19. Средства технической разведки.
20. Побочные излучения и наводки.
21. Государственная система защиты информации.
22. Источники функциональных сигналов. Фильтрация информационных сигналов.
23. Контроль эффективности инженерно-технической защиты информации.
24. Источники опасных сигналов (физические поля, электрические сигналы).
25. Методические рекомендации по оценке эффективности защиты информации.
26. Нормативные документы по противодействию технической разведке.
27. Моделирование инженерно-технической защиты информации.
28. Способы записи информации на различные виды носителей и принципы съема информации.
29. Средства предотвращения утечки информации по техническим каналам. Пространственное и линейное зашумление.
30. Основные демаскирующие признаки радиолокационных станций, лазерных излучений.
31. Средства инженерной защиты и технической охраны. Система охранно-тревожной сигнализации. Система контроля и управления доступом.
32. Особенности видовых признаков в видимом, инфракрасном и радиодиапазонах электромагнитных волн.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Классификация сигналов по форме, физической природе, виду информации и регулярности появления. Параметры сигналов.
35. Физические процессы подавления опасных сигналов.
36. Демаскирующие признаки веществ.
37. Методы инженерно-технической защиты информации.
38. Видовые, сигнальные и вещественные демаскирующие признаки. информационность признаков.
39. Каналы утечки информации за счет паразитных связей.
40. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.
41. Характеристика технической разведки.
42. Объект защиты, носитель информации, информационные процессы.
43. Показатели эффективности инженерно – технической защиты информации.
44. Организационно – технические мероприятия по защите информации
45. Свойства информации, влияющие на ее безопасность.
46. Виды защищаемой информации. защита информации от утечки, непреднамеренного и несанкционированного воздействия на нее.
47. Системный подход к защите информации.
48. Ценность информации.
49. Основные концептуальные положения инженерно-технической защиты информации.
50. Основные свойства информации как предмета защиты.
51. Технические средства защиты информации. Средства выявления каналов утечки информации.



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, знает схему лабораторной установки и принцип ее работы; 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, сдается 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 демонстрируются 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	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



	Авторы, составители	Заглавие	Издательство, год	Ресурс
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	Мищенко С. В., Мордасов Д. М., Мордасов М. М.	Физические основы технических измерений: учебное пособие (https://biblioclub.ru/index.php?page=book&id=277906)	Тамбов : Тамбовский государственный технический университет (ТГТУ), 2012	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Жигулин Г. П.	Организационное и правовое обеспечение информационной безопасности (https://e.lanbook.com/books/element.php?pl1_id=70952)	Санкт- Петербург : НИУ ИТМО, 2014	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	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

MS Office365

Notepad++

VirtualBox

Visual Studio

Adobe Connect Acrobat

LMS Moodle

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. 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.

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

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

4. 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, для выполнения курсовых работ, 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 технических средств защиты информации автоматизированных систем (аудитория 215 лабораторный корпус). Материально - техническое обеспечение приведено в паспорте лаборатории.

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)

Освоение содержания учебной дисциплины «Защита информации от утечки по техническим каналам» осуществляется на лекциях, лабораторных занятиях, а также 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 работы 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 работ. На лабораторных занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения учебной и производственной практик.

Самостоятельная работа студентов включает проработку лекционного курса, подготовку к лабораторным 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.

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 ассистивных 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 «EIBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеувеличители 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-PCM» 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:

- 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.

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) доступная форма предоставления инструкции по порядку проведения процедуры оценивания (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.

шифр: 10.05.01,
специализация N 1 "Анализ безопасности компьютерных систем",
специальность: Компьютерная безопасность,
название РПД: Защита информации от утечки по техническим каналам,
год набора: 2024,
форма обучения: очная

Проректор по учебной работе утверждено 21.02.24 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 9 от 15.02.2024

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры радиофизики и электроники

Протокол заседания № 05 от 23.01.2024

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) И.С. Зотов

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