

Документ подписан простой электронной подписью Информация о владельце: ФИО: Гаскаев Сергей Валерьевич Должность: Ректор	МИНОБРАЗОВАНИЯ И НАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	
Дата подписания: 04.04.2025 13:19:25 Уникальный программный ключ: 04c19ed8bfb98f516cb77a486b9a8788b8733737	Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»	стр. 1

Рабочая программа дисциплины (модуля)*

Криптографические протоколы

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 2022

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

Челябинск 2022 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

Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»	стр. 3
1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
Ознакомление студентов с основными понятиями теории криптографических протоколов;	
овладение основными идеями и методами современной теории криптографических протоколов;	
ознакомление студентов с основными криптографическими протоколами распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами;	
развитие навыка построения криптографического протокола из элементарных протоколов, и развития логического мышления в рамках этой задачи;	
овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола. овладение основными идеями и методами классической и современной криптографии, знакомство со средствами криптографической защиты информации, знание основополагающих документов в области защиты информации.	
Индикаторы достижения компетенций:	
ОПК-10.1. Обладает базовыми знаниями в области криптографии.	
ОПК-10.2. Демонстрирует умения использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	ФТД.01
2.1 Требования к предварительной подготовке обучающегося:	
Теория информации	
Языки программирования (дополнительные главы)	
Введение в специальность	
Математический анализ	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Преддипломная практика	
Методы и средства криптографической защиты информации	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	
Знать:	
Для достижения индикатора ОПК-10.1: Знать базовые понятия в области криптографии (протоколы обмена ключами, протоколы аутентификации (идентификации), протоколы доказательства с нулевым разглашением, протоколы электронной цифровой подписи, протоколы контроля целостности, протоколы электронных платежей, протоколы голосования).	
Уметь:	
Для достижения индикатора ОПК-10.2: Уметь использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	
Владеть:	
Для достижения индикатора ОПК-10.2: Владеть навыками использования средства криптографической защиты информации при решении задач профессиональной деятельности.	

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	классификацию шифров;
3.1.2	методы криптографического синтеза и анализа;
3.1.3	о применениях криптографии в решении задач аутентификации построения систем цифровой подписи
3.2	Уметь:
3.2.1	Использовать:
3.2.2	- типовые шифры замены и перестановки;
3.2.3	- требования к шифрам и основные характеристики шифров;

Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»		стр. 4
3.2.4	- принципы построения современных шифросистем;	
3.2.5	- типовые поточные и блочные шифры;	
3.2.6	- системы шифрования с открытыми ключами;	
3.2.7	- криптографические протоколы;	
3.2.8	- постановки задач криптоанализа и подходы к их решению	
3.3	Владеть:	
3.3.1	навыками использования основных типов шифров и криптографических алгоритмов;	
3.3.2	методами анализа простейших шифров;	
3.3.3	навыками математического моделирования в криптографии	

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	2 ЗЕТ
Часов по учебному плану: 72 в том числе: аудиторные занятия: 36 самостоятельная работа: 36	Виды контроля в семестрах: зачеты 6

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Криптографические протоколы			
1.1	Протоколы обмена ключами Протоколы аутентификации (идентификации) Протоколы доказательства с нулевым разглашением Протоколы электронной цифровой подписи Протоколы контроля целостности Протоколы электронных платежей Протоколы голосования /Пр/	6	36	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5
1.2	Подготовка к практической работе /Ср/	6	36	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по практическим работам.
Реферат
Зачет

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Собеседование по темам практических работ:

- 1) Протоколы обмена ключами.
- 2) Протоколы аутентификации (идентификации).
- 3) Протоколы доказательства с нулевым разглашением.
- 4) Протоколы электронной цифровой подписи.
- 5) Протоколы контроля целостности.
- 6) Протоколы электронных платежей.
- 7) Протоколы голосования.

Примерные темы реферата:

- 1) Протокол взаимоблокировки. Протокол Ву-Лама.
- 2) Протоколы обмена ключами.
- 3) Протокол Диффи-Хеллмана.
- 4) Протокол Kerberos.
- 5) Типичные атаки на протоколы аутентификации.
- 6) Протоколы защиты данных в сети Internet.
- 7) Протокол SSL(TLS).
- 8) Протокол Микали.
- 9) Стандарт X.509 и SPKI. Базовые архитектуры системуправления сертификатами.

<p>Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»</p>	<p>стр. 5</p>
<p>10) Схемы обязательств. 11) Схема Фейге-Фиата-Шамира. 12) Схема Гиллоу-Куискуотера. 13) Протокол Шаума-Педерсона. Неинтерактивный протокол Шаума-Педерсона. 14) Схемы разделения секрета. 15) Разделение секрета по схеме Асмута-Блума. 16) Контрольные проверки работоспособности применяемых криптографических средств защиты информации. 17) Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.</p>	
<p>6.3. Типовые контрольные вопросы и задания для промежуточной аттестации</p>	
<p>Вопросы к зачету: 1) Алгоритм Диффи-Хеллмана-Меркла. 2) Протокол ВВ84. 3) Парольная идентификация/аутентификация. 4) Протокол идентификации/аутентификации с использованием хеш-функции. 5) Протокол идентификации/аутентификации на основе шифрования с открытым ключом. 6) Сервер аутентификации Kerberos. 7) Идентификация/аутентификация с помощью биометрических данных. 8) Идентификационные карты и электронные ключи. 9) Схема на основе протокола с нулевым разглашением. 10) Протокол на базе алгоритма RSA. 11) Алгоритм цифровой подписи ГОСТ 34.10-94. 12) Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. 13) Разновидности ЭЦП. 14) Юридические основания использования ЭЦП. 15) Проверка четности. 16) Использование контрольных цифр. 17) Использование контрольных сумм. 18) Использование кодов Хэмминга. 19) Использование ЕСС. 20) Использование MAC-кодов. 21) Сущность и классификация денег. 22) Электронные платежи. 23) Традиционное («бумажное») голосование. 24) Упрощенный протокол голосования. 25) Протокол двух агентств Нурми-Саломая-Сантин. 26) Протоколы двух агентств Фудзикока-Окамото-Охта и Sensus. 27) Протокол голосования с одной Центральной комиссией на базе протокола ANDOS. 28) Протокол голосования с одной Центральной комиссией на базе «слепой» подписи.</p>	
<p>6.4. Критерии оценивания</p>	
<p>Критерии оценивания собеседования и отчета по практическим работам: В процессе выполнения практической работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование. Практическая 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 незначительные неточности в оформлении и ответах на вопросы. Практическая работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.</p> <p>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;</p>	

<p>Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»</p>	<p>стр. 6</p>
<p>- 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.</p> <p>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.).</p> <p>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.</p> <p>5) Грамотность (Макс. - 5 баллов) - отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; - отсутствие опечаток, сокращений слов, кроме общепринятых; - литературный стиль</p> <p>Реферат оценивается по 25 балльной шкале, балы переводятся в оценки успеваемости следующим образом: 15 баллов и выше - "зачтено" меньше 15 баллов - "незачтено"</p> <p>Критерии оценивания зачета: Студент допускается к зачету 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.</p> <p>Зачет проводится по билетам в устной форме. Студент выбирает билет в случайном порядке. Время подготовки студента для устного ответа на зачете должно составлять не менее 40 минут, время ответа – не более 20 минут. При подготовке и ответе на вопросы билета студент должен вести необходимые записи в листе устного ответа, который по окончании зачета подписывается студентом, сдается преподавателю и сохраняется им до окончания экзаменационной сессии. Проявленные студентом в ходе зачета знания оцениваются словами «зачтено», «не зачтено».</p> <p>«Зачтено» выставляется: 1) содержание материала билета раскрыто полностью; 2) материал изложен грамотно, в определенной логической последовательности, точно используется терминология; 3) показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; 4) продемонстрировано усвоение ранее изученных сопутствующих вопросов; 5) ответ самостоятельный, без наводящих вопросов; 6) допущены одна–две неточности при освещении второстепенных вопросов, которые исправляются после замечаний или наводящих вопросов.</p> <p>«Не зачтено» выставляется: 1) не раскрыто основное содержание учебного материала; 2) обнаружено незнание или непонимание большей или наиболее важной части учебного материала; 3) допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.</p>	

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	Фороузан Б. А.	Математика криптографии и теория шифрования: учебное пособие (https://biblioclub.ru/index.php?page=book&id=428998)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.2	Лापони́на О. Р.	Криптографические основы безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429092)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»				стр. 7
	Авторы, составители	Заглавие	Издательство, год	Ресурс
ЛП.3	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие (https://biblioclub.ru/index.php?page=book&id=493059)	Таганрог : Южный федеральный университет, 2016	ЭБС
ЛП.4	Бабаш А.В.	Криптографические методы защиты информации: учебно-методическое пособие: том 3 (http://znanium.com/catalog/document?id=52118)	Москва : Издательский Центр РИОР, 2014	ЭБС
ЛП.5	Петров А. А.	Компьютерная безопасность. Криптографические методы защиты (http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3027)	Москва : ДМК Пресс, 2008	ЭБС
ЛП.6	Бабаш А.В.	Криптографические методы защиты информации: учебно-методическое пособие: том 1 (http://znanium.com/catalog/document?id=368272)	Москва : Издательский Центр РИОР, 2021	ЭБС
7.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Ресурс
ЛП.1	Василенко О. Н.	Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное): монография (https://biblioclub.ru/index.php?page=book&id=61814)	Москва : МЦНМО, 2006	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				
MS Office365				
Adobe Reader				
WinDjView				
LMS Moodle				
Adobe Connect Acrobat				
Антивирус Касперского				
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.				

Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»	стр. 8
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Для реализации дисциплины используются учебные аудитории 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 семинарского типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий (мультимедийные презентации).	
Практические 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)
<p>Освоение содержания учебной дисциплины «Криптографические протоколы» осуществляется на практических занятиях и в процессе самостоятельной учебной деятельности студентов.</p> <p>Практические занятия предназначены для приобретения опыта практической реализации полученных теоретических знаний. Необходимый уровень подготовки контролируется преподавателем перед проведением практических занятий. На практических занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения учебной и производственной практик.</p> <p>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.).</p> <p>При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.</p> <p>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 применяться компоненты, не входящие в перечень электронной информационно-образовательной среды.</p>

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ
<p>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.</p> <ol style="list-style-type: none"> 1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraille-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. <p>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).</p>

<p>Рабочая программа дисциплины "Криптографические протоколы" по направлению подготовки (специальности) "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»</p>	<p>стр. 9</p>
<p>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.</p> <p>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 CleVu с большими кнопками и с разделяющей клавиши накладкой).</p> <p>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:</p> <p>Для лиц с нарушениями зрения:</p> <ul style="list-style-type: none"> - в печатной форме увеличенным шрифтом, - в форме электронного документа, - в форме аудиофайла, - в печатной форме шрифтом Брайля. <p>Для лиц с нарушениями слуха:</p> <ul style="list-style-type: none"> - в печатной форме, - в форме электронного документа. <p>Для лиц с нарушениями опорно-двигательного аппарата:</p> <ul style="list-style-type: none"> - в печатной форме, - в форме электронного документа, - в форме аудиофайла. <p>Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 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). <p>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.</p> <p>Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.</p>	

Рабочая программа дисциплины (модуля) одобрена и рекомендована:

Проректор по учебной работе утверждено 30.05.2022 В.Е. Федоров

Ученым советом физического факультета

Протокол заседания № 07 от 28.04.2022

Председатель Ученого совета
физического факультета

согласовано

Д.А. Захаревич

Заседанием кафедры радиофизики и электроники

Протокол заседания № 09 от 19.04.2022

Заведующий кафедрой

согласовано

А.В. Бутаков

Автор (составитель)

А.В. Бутаков

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