Рабочая программа дисциплины (модуля)*

Защита web-приложений

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(ы) набора 2023

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

Челябинск 2023 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является:

обучение студентов принципам обнаружения уязвимостей в web-приложениях и методам защиты от них.

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах).

УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном (ых) языке(ах)

УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке (ах).

ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем; о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации.

ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей.

ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.03.07

2.1 Требования к предварительной подготовке обучающегося:

Информатика

Аппаратные средства вычислительной техники

Алгебра

Модели безопасности компьютерных систем

Методы программирования

Компьютерные сети

Web-программирование

Беспроводные сети

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

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Знать:

– основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий.

Уметь:

– составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов.

Владеть:

– иметь навыки вербальной коммуникации на техническом иностранном языке.

ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web- приложениях

Знать:

– основы политики безопасности компьютерных систем;
– алгоритмы разработки технических заданий на создание средств защиты информации;
– определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети;
– требования к защите информации компьютерной системы;
– алгоритмы разработки руководящих документов по защите информации.

Уметь:

– анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;
– разрабатывать профили защиты компьютерных систем;
– формулировать задания по безопасности компьютерных систем;
– выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации;
– формировать политики безопасности компьютерных систем и сетей.

Владеть:

– навыками использования средств защиты информации;
– навыками использования нормативных правовых актов в области защиты информации;
– навыками разработки руководящих документов по защите информации.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные термины, употребляющиеся в сфере защиты web-приложений;
3.1.2	– классы атак на web-приложения, методы защиты от них.
3.1.3	
3.2	**Уметь:**
3.2.1	– использовать изученные механизмы защиты от распространенных атак.
3.3	**Владеть:**
3.3.1	– анализа исходных кодов, настроек конфигурации с целью обнаружения web-уязвимостей.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**6 ЗЕТ**
Часов по учебному плану : 216 в том числе : аудиторные занятия : 68 самостоятельная работа : 101 часов на контроль : 36 контактная работа: 79 ИКР: 11	Виды контроля в семестрах: экзамены 10

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основы безопасности web-приложений			
1.1	Объекты web-сервисов. Проблемы безопасности web-клиентов. Методы взлома web-приложений. Сценарии компьютерных атак. Системы обнаружения вторжений, фаерволлы, используемые в web- технологиях. /Лек/	10	8	Л1.1 Л1.2 Л1.3Л2.1

1.2	Объекты web-сервисов. Проблемы безопасности web-клиентов. Методы взлома web-приложений. Сценарии компьютерных атак. Системы обнаружения вторжений, фаерволлы, используемые в web- технологиях. /Пр/	10	8	Л1.1 Л1.2 Л1.3Л2.1
1.3	Основы безопасности web-приложений. Проработка лекционного материала. /Ср/	10	30	Л1.1 Л1.2 Л1.3Л2.1
	Раздел 2. Атаки на web-приложения			
2.1	Классы атак. Уязвимости аутентификации. Brute Froce. Недостаточная аутентификация. Небезопасное восстановление паролей. Атаки типа «Credential/Session Prediction», «Insufficient Authorization», «Insufficient Session Expiration», «Session Fixation». Атаки на клиентов. Подмена содержимого. Межсайтовое исполнение сценариев. Расщепление HTTP-запроса. Атака на функции форматирования строк. Переполнение буфера. Внедрение операторов LDAP. Выполнение команд ОС. Внедрение операторов SQL. Слепые инъекции. Внедрение серверных сценариев SSI. Внедрение операторов XPath. Идентификация web-приложений. Information Leakage. Path Traversal. Предсказуемое расположение ресурсов. Злоупотребление функциональными возможностями. Отказ в обслуживании. Флудинг. Cross Site Request Forgery. /Лек/	10	14	Л1.1 Л1.2 Л1.3Л2.1
2.2	Классы атак. Уязвимости аутентификации. Brute Froce. Недостаточная аутентификация. Небезопасное восстановление паролей. Атаки типа «Credential/Session Prediction», «Insufficient Authorization», «Insufficient Session Expiration», «Session Fixation». Атаки на клиентов. Подмена содержимого. Межсайтовое исполнение сценариев. Расщепление HTTP-запроса. Атака на функции форматирования строк. Переполнение буфера. Внедрение операторов LDAP. Выполнение команд ОС. Внедрение операторов SQL. Слепые инъекции. Внедрение серверных сценариев SSI. Внедрение операторов XPath. Идентификация web-приложений. Information Leakage. Path Traversal. Предсказуемое расположение ресурсов. Злоупотребление функциональными возможностями. Отказ в обслуживании. Флудинг. Cross Site Request Forgery. /Пр/	10	14	Л1.1 Л1.2 Л1.3Л2.1
2.3	Атаки на web-приложения. Проработка лекционного материала и материала практических занятий. /Ср/	10	36	Л1.1 Л1.2 Л1.3Л2.1
	Раздел 3. Защита web-приложений			
3.1	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений /Лек/	10	12	Л1.1 Л1.2 Л1.3Л2.1
3.2	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений. /Пр/	10	12	Л1.1 Л1.2 Л1.3Л2.1
3.3	Администрирование web-серверов. Обработка входных данных. Анализаторы исходных кодов. Web application firewall. Фильтрация sql-запросов. Параметризованные запросы. Сканеры web- приложений. Проработка лекционного материала и материала практических занятий. /Ср/	10	35	Л1.1 Л1.2 Л1.3Л2.1
	Раздел 4. Экзамен			
4.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	10	11	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Устный опрос.
Самостоятельная работа.
Перечень вопросов к экзамену.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса для текущей аттестации
1. Основные принципы проведения аудита информационной безопасности web-приложений.
2. Стандарты безопасности web-приложений.
3. Этапы проведения аудита информационной безопасности web-приложений.
4. Принципы построения защищенных web-приложений.
5. Модели угроз безопасности web-приложений.
6. Классы компьютерных атак на web-приложения.
7. Общие понятия об информационным системах, построенных с использованием web-технологий.
8. Виды атак на клиентов web-приложений.
9. SQL-инъекции.
10. Уязвимости типа "file upload".
11. Удаленное подключение файлов.
12. Исполнение кода.
13. Сканеры информационной безопасности.
14. Структура web-сервиса.
15. Безопасность web-клиентов.
16. Системы обнаружения вторжений.
17. Web-фаерволлы.
18. Классы атак на web-приложения.
19. Виды атак на протоколы аутентификации.
20. Виды атак на протоколы авторизации.
21. Уязвимости по подмене содержимого.
22. Атаки на web-клиентов.
23. Межсайтовое исполнение сценариев.
24. Расщепление HTTP-запроса.
25. Понятие и защита от SQL-инъекций.
26. Основные виды SQL-инъекций.
27. Слепые SQL-инъекции, методы обнаружения и защиты.
28. Уязвимости по раскрытию информации.
29. Логические уязвимости web-приложений.
30. Основные правила администрирования web-серверов.
31. Методы анализа исходных кодов web-приложений.
32. Правила обработки входных данных.

Перечень самостоятельных работ
1. Тестирование системы аутентификации.
2. Тестирование системы авторизации.
3. Исследование компьютерных атак на клиентов web-приложений.
4. Исследование компьютерных атак типа SQL-инъекция.
5. Исследование уязвимостей web-сервисов по загрузке файлов.
6. Исследование уязвимостей по удаленному подключению файлов.
7. Исследование уязвимостей по удаленному исполнению кода.
8. Использование сканеров информационной безопасности.
9. Использование анализаторов программного кода.
10. Реферат на тему "Аудит безопасности web-сервера".

Полные тексты самостоятельных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Список вопросов к экзамену
1. Структура web-сервиса.
2. Безопасность web-клиентов.
3. Системы обнаружения вторжений.
4. Web-фаерволлы.

5. Классы атак на web-приложения.
6. Виды атак на протоколы аутентификации.
7. Виды атак на протоколы авторизации.
8. Уязвимости по подмене содержимого.
9. Атаки на web-клиентов.
10. Межсайтовое исполнение сценариев.
11. Расщепление HTTP-запроса.
12. Понятие и защита от SQL-инъекций.
13. Основные виды SQL-инъекций.
14. Слепые SQL-инъекции, методы обнаружения и защиты.
15. Уязвимости по раскрытию информации.
16. Логические уязвимости web-приложений.
17. Атаки по исполнению кода на стороне сервера.
18. Основные правила администрирования web-серверов.
19. Методы анализа исходных кодов web-приложений.
20. Понятие и назначение WAF.
21. Правила обработки входных данных.

6.4. Критерии оценивания

В течение семестра студент должен выполнить десять самостоятельных работ, каждая из которых оценивается в 5 баллов.
Максимальный балл за самостоятельную работу – 15 баллов.
Максимальное количество баллов за самостоятельные работы за семестр – 50.
Допуском до проведения экзамена являются сданные студентом самостоятельные работы в течение семестра.
Экзамен проводится в два этапа. На первом студент отвечает на два вопроса. На втором студент проводит аудит безопасности учебного веб-сервера и готовит по результатам отчет. Продолжительность – 90 минут.
Максимальный балл за ответ на теоретический вопрос – 15 баллов.
Максимальный балл за практическую часть экзамена – 20 баллов.

Сводная таблица рейтинга успеваемости

№	Вид оценочного средства	Максимальное кол-во баллов
1	Самостоятельная работа №1-10	10x5=50
2	Экзамен (теоретический вопрос)	2x15=30
3	Экзамен (практическая часть)	20
Итого		100

Критерии оценивания теоретического вопроса экзамена
Максимальный балл за ответ на теоретический вопрос – 15 баллов.
Отлично/зачтено/12-15 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.
Хорошо/зачтено/8-11 баллов - Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует логичность и последовательность. Однако допускается неточность.
Удовлетворительно/зачтено/4-7 баллов - Студентом дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа.
Неудовлетворительно/не зачтено/0-3 балла - Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Критерии оценивания практической части экзамена
Максимальный балл за практическую часть зачета – 20 баллов.
Отлично/зачтено/15-20 баллов - Студентом подготовлен полный отчет об обнаружении по результатам аудита трех

уникальных уязвимостей веб-сервера, изложены их описание, способы эксплуатации и устранения угроз безопасности.
Хорошо/зачтено/11-14 баллов - Студентом подготовлен полный отчет об обнаружении по результатам аудита двух уникальных уязвимостей веб-сервера, изложены их описание, способы эксплуатации и устранения угроз безопасности.
Удовлетворительно/зачтено/7-10 баллов - Студентом подготовлен полный отчет об обнаружении по результатам аудита одной уникальной уязвимости веб-сервера, изложены ее описание, способы эксплуатации и устранения угроз безопасности.
Неудовлетворительно/не зачтено/0-6 баллов - Студентом подготовлен отчет, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области.

Критерии оценки самостоятельной работы
Максимальный балл за самостоятельную работу – 5 баллов.
5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
2 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.
0 баллов – не выполнена самостоятельная работа.

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.
В течение семестра проводятся самостоятельные работы по одному из рассматриваемых разделов, которые осуществляют срез знаний по основным понятиям, определениям и задачам.
Для экзамена:
0-54 баллов - неудовлетворительно (2);
64-74 баллов - удовлетворительно (3);
75-90 баллов - хорошо (4);
91-100 баллов - отлично (5).

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	Скембрей, Шема, Чекатков А. А.	Секреты хакеров. Безопасность Web-приложений - готовые решения	М. : Вильямс, 2003	
Л1.2	Форристал Д., Брумс К., Симонис Д., Бегнолл Б.	Защита от хакеров Web-приложений (https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1116)	Москва : ДМК Пресс, 2008	ЭБС
Л1.3	Скрыпников А. В., Арапов Д. В., Денисенко В. В., Герасимова Т. Д.	Защита Web-приложений: учебное пособие (https://biblioclub.ru/index.php?page=book&id=612405)	Воронеж : Воронежский государственный университет инженерных технологий, 2020	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Марухленко А. Л., Марухленко Л. О., Ефремов М. А.	Разработка защищённых интерфейсов Web-приложений: учебное пособие (https://biblioclub.ru/index.php?page=book&id=599050)	Москва, Берлин : Директ-Медиа, 2021	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

Notepad++

VirtualBox

Visual Studio

NetBeans

Python

Ubuntu Linux

MySQL

PostgreSQL

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Лабораторные занятия проходят в учебных лабораториях технических средств защиты информации и "Сетевой полигон" (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

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

При изучении данной дисциплины используются лекционные и практические занятия, самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях рассматриваются проблемы безопасности web-клиентов, методы взлома web-приложений, сценарии компьютерных атак, администрирование web-серверов и др.

Рекомендуется перед каждым лекционным и практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и 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:
- 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.

Специальность 10.05.01 Компьютерная безопасность
Специализация № 1 «Анализ безопасности компьютерных систем»
Рабочая программа дисциплины «Защита web-приложений»
2023 год набора, очная форма обучения

Проректор по учебной работе утверждено 24.04.2023 В.Е. Федоров

Ученым советом математического факультета

Протокол заседания № 8 от 13.04.2023

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 10 от 31.03.2023

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

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