


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы



Буинцев Д.Н.

«_24_» сентября 2024 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.В.07 «Безопасность Web-приложений»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

Бакалавр

Форма обучения

очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Б1.В.07 Безопасность Web-приложений составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

Вашакидзе Н.С., старший преподаватель кафедры информатики



Рабочая программа дисциплины Б1.В.07 Безопасность Web-приложений утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности
заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Целями освоения дисциплины Безопасность Web-приложений является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов системного и аналитического мышления, формирование у студентов знаний об основных типах атак на веб-приложения и методах их предотвращения.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных элементов и механизмов веб-приложений (протокол HTTP, модель DOM, политика SOP, веб-браузеры, веб-серверы, балансировщики нагрузки);
- – изучение основных видов атак на веб-приложения: XSS, SQL, CSRF, IDOR и др.
- – приобретение навыков обнаружения и защиты от атак рассматриваемых классов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность Web-приложений» относится к части, формируемой участниками образовательных отношений Блока 1, Дисциплины (модули) (Б1.В.07) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знании следующих дисциплин: Операционные системы, Web-технологии, языки и средства создания web-приложений.

Постреквизиты дисциплины:

Основные положения данной дисциплины выступают опорой для дисциплин: Методы и средства криптографической защиты информации, дисциплин по выбору, призваны подготовить к прохождению учебной и производственной практик, к научно-исследовательской работе.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-3	Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем	ПКС-3.1 - Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; ПКС-3.2 - Умеет определять подлежащие защите информационные ресурсы автоматизированных систем; ПКС-3.3 - Владеет навыками анализа угрозы автоматизированной системе и циркулирующей в ней информации, выбора необходимых средства для обеспечения информационной безопасности.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **3** зачетные единицы (**108** академических часов).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	5	
Общая трудоемкость	108	108
Контактная работа:	58	58
Лекции (Лек)	18	24
Лабораторные работы (Лаб)	36	30
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	4	4
Контактная работа в период промежуточной аттестации (КонтПА)		0
Промежуточная аттестация – зачет		0
Самостоятельная работа:	50	50
- самостоятельное изучение разделов (перечислить);	0	0
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	14	14
- подготовка к лабораторным занятиям;	30	30
- подготовка к коллоквиумам;	2	2
- подготовка к промежуточной аттестации и т.п.)	4	4

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы		Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Архитектура веб-приложений.	5	2	0	2	6	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2. Поиск уязвимостей к атакам CSRF.		2	0	4	6	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3. Поиск уязвимостей к атакам XSS.		2	0	6	8	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Тема 4. Поиск уязвимостей к атакам SQL.		4	0	8	8	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Тема 5. Отказ в обслуживании (DoS)		4	0	8	8	Устный опрос по теме лекции. Проверка домашнего задания.
6.	Тема 6. Эксплуатация сторонних зависимостей		4		8	8	Устный опрос по теме лекции. Проверка домашнего задания.
	коллоквиумы					2	Собеседование
	зачет				4	Устный зачет (по билетам)	
	Итого:	104	18	0	36	50	

4.3. Содержание разделов дисциплины

Тема 1. Архитектура веб-приложений

Обзор современных клиентских (Frontend) и серверные (Backend) фреймворков для создания веб-приложений. Сравнение современных и более ранних версий приложений. Системы аутентификации и авторизации. Веб-серверы. Хранение данных на стороне сервера и на стороне клиента. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.

Тема 2. Поиск уязвимостей к атакам CSRF

Понятие CSRF атаки. Влияние уязвимости CSRF на пользователя. Способы защиты от CSRF. Использование csurf-библиотеки. Инициализация CSRF-токена. Валидация CSRF-токена. Реализация CSRF-токена. Недостатки CSRF. Защита от CSRF. Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния. Противодействие CRSF на уровне кода. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.

Тема 3. Поиск уязвимостей к атакам XSS.

Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS. XSS-атака на базе DOM. XSS с мутациями. Приемы написания кода для противодействия XSS. Очистка пользовательского ввода. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML

Тема 4. Поиск уязвимостей к атакам SQL

Внедрение SQL-кода. Внедрение кода. Внедрение команд. Противодействие внедрению.297

Противодействие внедрению SQL-кода. Распознавание внедрения SQL-кода. Подготовленные операторы. Более специфические методы защиты. Защита от других видов внедрения. Потенциальные цели внедрения. Принцип минимальных привилегий. Белый список команд.

Тема 5. Отказ в обслуживании (DoS)

ReDoS атака. Логические DoS-уязвимости. Распределенная DoS-атака. Противодействие DoS-атакам. Противодействие атакам ReDoS. Защита от логических DoS-атак. Защита от DDoS. Смягчение DDoS-атак.

Тема 6. Эксплуатация сторонних зависимостей

Методы интеграции. Ветви и вилки. Приложения с собственным сервером. Интеграция на уровне кода. Диспетчеры пакетов. JavaScript. Java. Другие языки. База данных общеизвестных уязвимостей. Защита сторонних зависимостей. Оценка дерева зависимостей. Моделирование дерева зависимости. Деревья зависимостей на практике. Автоматизированная оценка. Техники безопасной интеграции. Разделение интересов. Безопасное управление пакетами.

4.4 Темы и планы лабораторных занятий

Лабораторное занятие №1 (2 ч.)

Тема Архитектура веб-приложений

Вопросы для обсуждения:

1. Обзор современных клиентских (Frontend) и серверные (Backend) фреймворков для создания веб-приложений.
2. Сравнение современных и более ранних версий приложений.
3. Системы аутентификации и авторизации.
4. Веб-серверы.
5. Хранение данных на стороне сервера и на стороне клиента.
6. Обнаружение сторонних зависимостей.

7. Поиск слабых мест в архитектуре приложения.

Лабораторное занятие №2 (4 ч.)

Тема Поиск уязвимостей к атакам CSRF

Вопросы для обсуждения:

1. Понятие CSRF атаки.
2. Влияние уязвимости CSRF на пользователя.
3. Способы защиты от CSRF.
4. Использование csurf-библиотеки.
5. Инициализация CSRF-токена.
6. Валидация CSRF-токена.
7. Реализация CSRF-токена.
8. Недостатки CSRF.
9. Защита от CSRF.
10. Проверка заголовков. CSRF-токен.
11. CSRF-токены без сохранения состояния.
12. Противодействие CRSF на уровне кода.
13. Запросы GET без сохранения состояния.
14. Снижение риска CSRF на уровне приложения.

Лабораторное занятие №3 (6 ч.)

Тема 3. Поиск уязвимостей к атакам XSS.

Вопросы для обсуждения:

1. Обнаружение XSS-уязвимости.
2. Хранимый XSS.
3. Отраженный XSS.
4. XSS-атака на базе DOM.
5. XSS с мутациями.
6. Приемы написания кода для противодействия XSS.
7. Очистка пользовательского ввода.
8. Приемник DOMParser. Приемник SVG. Приемник Blob.
9. Санация гиперссылок. Символьные сущности в HTML

Лабораторное занятие №4 (8 ч.)

Тема Поиск уязвимостей к атакам SQL

Вопросы для обсуждения:

1. Внедрение SQL-кода.
2. Внедрение кода.
3. Внедрение команд.
4. Противодействие внедрению.
5. Противодействие внедрению SQL-кода.
6. Распознавание внедрения SQL-кода.
7. Подготовленные операторы.
8. Более специфические методы защиты.
9. Защита от других видов внедрения.
10. Потенциальные цели внедрения.
11. Принцип минимальных привилегий.
12. Белый список команд.

Лабораторное занятие №5 (8 ч.)

Тема Отказ в обслуживании (DoS)

Вопросы для обсуждения:

1. ReDoS атака.
2. Логические DoS-уязвимости.
3. Распределенная DoS-атака.
4. Противодействие DoS-атакам.
5. Противодействие атакам ReDoS.
6. Защита от логических DoS-атак.
7. Защита от DDoS. Смягчение DDoS-атак.

Лабораторное занятие №6 (8 ч.)

Тема Эксплуатация сторонних зависимостей

Вопросы для обсуждения:

1. Методы интеграции.
2. Ветви и вилки.
3. Приложения с собственным сервером.
4. Интеграция на уровне кода.
5. Диспетчеры пакетов.
6. JavaScript. Java. Другие языки.
7. База данных общеизвестных уязвимостей.
8. Защита сторонних зависимостей.
9. Оценка дерева зависимостей.
10. Моделирование дерева зависимости.
11. Деревья зависимостей на практике.
12. Автоматизированная оценка.
13. Техники безопасной интеграции.
14. Разделение интересов.
15. Безопасное управление пакетами.

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	1 семестр		
1.	Тема 1. Архитектура веб-приложений.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Тема 2. Поиск уязвимостей к атакам CSRF.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Тема 3. Поиск уязвимостей к атакам XSS.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в

			компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Тема 4. Поиск уязвимостей к атакам SQL.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
5.	Тема 5. Отказ в обслуживании (DoS)	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
6.	Тема 6. Эксплуатация сторонних зависимостей	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Примерные вопросы к зачету

1. Сравнение современных и более ранних версий приложений. Системы аутентификации и авторизации.
2. Веб-серверы. Хранение данных на стороне сервера и на стороне клиента.
3. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.
15. Понятие CSRF атаки. Влияние уязвимости CSRF на пользователя.
16. Способы защиты от CSRF. Использование csurf-библиотеки. Инициализация CSRF-токена.
17. Валидация CSRF-токена. Реализация CSRF-токена.
18. Недостатки CSRF. Защита от CSRF.
19. Проверка заголовков. CSRF-токен. CSRF-токены без сохранения состояния.
20. Противодействие CRSF на уровне кода.
21. Запросы GET без сохранения состояния. Снижение риска CSRF на уровне приложения.
22. Обнаружение XSS-уязвимости. Хранимый XSS. Отраженный XSS.
23. XSS-атака на базе DOM. XSS с мутациями. Приемы написания кода для противодействия XSS.
24. Очистка пользовательского ввода.
25. Приемник DOMParser. Приемник SVG. Приемник Blob. Санация гиперссылок. Символьные сущности в HTML
26. Внедрение SQL-кода. Внедрение кода. Внедрение команд.
27. Противодействие внедрению SQL-кода. Распознавание внедрения SQL-кода.
28. Подготовленные операторы. Более специфические методы защиты. Защита от других видов внедрения.
29. Потенциальные цели внедрения. Принцип минимальных привилегий.
30. ReDoS атака. Логические DoS-уязвимости. Распределенная DoS-атака.
31. Противодействие DoS-атакам. Противодействие атакам ReDoS.

32. Защита от логических DoS-атак. Защита от DDoS. Смягчение DDoS-атак.
33. Методы интеграции. Ветви и вилки. Приложения с собственным сервером.
34. Интеграция на уровне кода. Диспетчеры пакетов.
35. База данных общеизвестных уязвимостей.
36. Защита сторонних зависимостей. Оценка дерева зависимостей.
37. Моделирование дерева зависимости. Деревья зависимостей на практике.
38. Автоматизированная оценка. Техники безопасной интеграции.
39. Разделение интересов. Безопасное управление пакетами.

8. Система оценивания планируемых результатов обучения

Критерии оценивания

Оценка «зачтено» выставляется:

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр /экзамен			60	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539995>
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионально-го образования / С. А. Нестеров. — Москва : Изда-тельство Юрайт, 2019. — 321 с. — (Профессиональ-ное образование). — ISBN 978-5-534-07979-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/442312>
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов О. В. Казарин, А. С.

Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/538066>

9.2. Дополнительная литература

1. Пособие по практическим занятиям: учеб.-метод. пособие / сост.: А.К. Большев, И.А. Юшкевич. - СПб. – 2016
2. [<https://lk.etu.ru/dashboard/api/download/1182>]
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543631>

9.3. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
15. Visual Studio Professional
16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление);
17. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
18. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)

3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.nt.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Polpred.com Обзор СМИ (<http://polpred.com/>)
15. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
16. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
17. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
18. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме

на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).