Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«01» 06 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность веб-приложений

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС – Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

к.ф.-м.н., доцент _____ Лошманов А.Ю.
(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой
ИБАС _____ Лошманов А.Ю.
(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Безопасность веб-приложений» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1509, и образовательной программы подготовки специалистов «Информационная безопасность автоматизированных систем» (10.05.03) уровень специалитета, специализация «Обеспечение информационной безопасности распределенных информационных систем».

Задачи дисциплины	Обеспечить освоение основ: • проводить анализ и выполнять последовательное тестирование всех способов атаки на веб-приложений по классификации OWASP Top 10.
Основные разделы / темы дисциплины	1. Концепции веб-сайтов 2. Инъекции 3. Взлом аутентификации и сеанса 4. Утечка важных данных 5. Внешние XML объекты 6. Нарушение контроля доступа 7. Небезопасная конфигурация 8. Межсайтовый скриптинг (XSS) 9. Небезопасная десериализация 10. Использование компонентов с известными уязвимостями 11. Отсутствие журналирования и мониторинга

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Безопасность веб-приложений» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
ОПК-4: способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	З(ОПК-4) основных подходов к поиску информации в компьютерных системах, сетях, библиотечных фондах	У(ОПК-4) использовать ЭВМ для поиска информации в компьютерных системах, сетях, библиотечных фонда	Н(ОПК-4) поиска информации в компьютерных системах, сетях, библиотечных фондах

ПК-1: способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	З(ПК-1) методов поиска, изучения систематизации и обобщения информации на иностранном языке	У(ПК-1) осуществлять поиск, изучение, обобщение и систематизацию информации на иностранном языке	Н(ПК-1) работы с научно-технической информацией, нормативными и методическими материалами в сфере профессиональной деятельности на иностранном языке

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Безопасность веб-приложений» изучается на 4 курсе в 8 семестре.

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к вариативной части.

Дисциплина «Безопасность веб-приложений»» основывается на знаниях, умениях и навыках, полученных при изучении дисциплин по выбору: «Анализ защищенности распределенных информационных систем».

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 з.е., 108 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	48
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-	60

Объем дисциплины	Всего академических часов
образовательной среде вуза	
Промежуточная аттестация обучающихся – Зачет с оценкой	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Концепции веб-сайтов. Принципы работы веб-серверов и веб-приложений. Принципы безопасности веб-сайтов и веб-приложений. Что такое OWASP. Обзор классификации OWASP Top 10. Знакомство с инструментами для выполнения атак. Настройка лаборатории	2		3	5
Инъекции. Что такое инъекции и почему они становятся возможными. Не SQL инъекции. Простые SQL инъекции. Слепые SQL инъекции	1		3	5
Взлом аутентификации и сеанса. Атаки на аутентификацию. Атаки на управление сеансом	1		3	5
Утечка важных данных. Принципы атак, приводящих к утечке данных	1		3	5
Внешние XML объекты. Что такое внешние объекты XML (XXE). Принципы атак на внешние объекты XML	2		3	5
Нарушение контроля доступа. Концепции DOR. Принципы атак на функциональный уровень. Что такое обход каталога. Предназначение заголовка хоста в HTTP. Концепции подключения локального или удаленного файла. Другие возможности ограничения доступа. Что такое подделка запросов на стороне сервера (SSRF). Что такое внешние объекты XML (XXE)	2		3	5
Небезопасная конфигурация. Принципы атак на конфигурацию. Произвольный доступ к файлам в Samba. Файл междоменной	2		3	5

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
политики Flash. Общие ресурсы в AJAX. Межсайтовая трассировка (XST)				
Межсайтовый скриптинг (XSS). Концепции XSS. Отраженные XSS. Что такое JSON. Что такое AJAX. Что такое функция Eval. Что такое атрибут HREF. Что такое phpMyAdmin. Хранимые XSS	2		3	5
Небезопасная десериализация. Что такое сериализация и десериализация. Принципы атак на небезопасную десериализацию	1		3	5
Использование компонентов с известными уязвимостями. Концепции инвентаризации уязвимостей. Что такое переполнение буфера	1		3	5
Отсутствие журналирования и мониторинга. Концепции журналирования в веб-приложениях	1		2	5
РГР				5
ИТОГО по дисциплине	**16**		**32**	**60**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	25
Подготовка к занятиям семинарского типа	30
Подготовка и оформление РГР	5
	60

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для

оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 5).

Таблица 5 – Технологическая карта

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	1 неделя семестра	10 баллов	10 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 6 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
2	Лабораторная работа 2	2 – 3 недели семестра	10 баллов	
3	Лабораторная работа 3	4 неделя семестра	10 баллов	
4	Лабораторная работа 4	5 - 6 недели семестра	10 баллов	
5	Лабораторная работа 5	7 неделя семестра	10 баллов	
6	Лабораторная работа 6	8 неделя семестра	10 баллов	
7	Лабораторная работа 7	9 неделя семестра	10 баллов	

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
8	Лабораторная работа 8	10 неделя семестра	10 баллов	
9	Лабораторная работа 9	11 неделя семестра	10 баллов	
10	Лабораторная работа 10	12 неделя семестра	10 баллов	
11	Лабораторная работа 11	13 неделя семестра	10 баллов	
12	Расчетно-графическая работа	14 – 16 недели семестра	10 баллов	10 баллов – студент правильно и полностью выполнил задание. Показал отличные знания, умения и навыки в рамках освоенного учебного материала. 7 баллов – студент выполнил задание с неточностями и/или не полностью. Показал хорошие знания, умения и навыки в рамках освоенного учебного материала. 4 балла - студент выполнил задание не в срок. Показал удовлетворительные знания, умения и навыки в рамках освоенного учебного материала. 0 баллов – задание не выполнено
ИТОГО Текущий контроль:		-	120 баллов	-
Критерии оценки результатов обучения по дисциплине: 0 – 64% от максимально возможной суммы баллов – «неудовлетворительно»				

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
(недостаточный уровень для промежуточной аттестации по дисциплине); 65-74% от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75-84% от максимально возможной суммы баллов – «хорошо» (средний уровень); 85-100% от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

Задания для текущего контроля

Лабораторные работы (11 штук)

1. Установка, настройка и запуск учебного сайта
2. Выполнение атак на учебный веб-сайт с применением инъекций и защита сайта от таких атак.
3. Выполнение атак на учебный веб-сайт с применением атак на аутентификацию и управление сеансом.
4. Выполнение атак на учебный веб-сайт с применением техник раскрытия чувствительных данных и защита сайта от таких атак.
5. Выполнение XXE атак на учебном веб-сервере и защита.
6. Выполнение атак на функционал учебного веб-сервера и защита.
7. Выполнение атак на конфигурацию учебного веб-сервера и защита от таких атак.
8. Выполнение атак на учебный веб-сайт с помощью отраженных и хранимых XSS и защита сайта от таких атак.
9. Выполнение атак на учебный веб-сайт с уязвимостью небезопасной десериализации и защита сайта от таких атак.
10. Выполнение атак на учебный веб-сервер с использованием эксплойтов на известные уязвимости и защита сервера от таких атак.
11. Изучение концепций и практических примеров отсутствия журналирования и мониторинг.

Примерные темы РГР

1. Провести XXE атаки на учебном веб-сервере и защита.
2. Управление жесткими дисками - системная утилита Paragon Partition Manager
3. Резервное копирование и восстановление данных - системная утилита Paragon Drive Backup Professional

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем: учеб. пособие / В.А.Челухин. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2014. – 207 с. (в библиотеке имеется 45 экз.)

2.Боженюк, А. В. Интеллектуальные интернет-технологии / А.В. Боженюк, Э.М. Котов, А.А. Целых. - М.: Феникс, 2015. - 384 с.

3.Герасевич, Виталий Блоги и RSS: интернет-технологии нового поколения / Виталий Герасевич. - М.: БХВ-Петербург, 2015. - 256 с.

8.2 Дополнительная литература

1. Купко, Д. Знакомство в Интернете / Д. Купко. - М.: СПб: Питер, 2014. - 160 с.

2. Ли, Чарлин Взрывная Web_Волна. Как добиться успеха в мире, преображенном интернет-технологиями / Чарлин Ли , Джош Бернофф. - М.: Альпина Паблишер, Юрайт, 2014. - 280 с..

3. Мураховский, В.И. Интернет у Вас дома / В.И. Мураховский, С.В. Симонович. - М.: АСТ-Пресс, 2013. - 432 с.

8.3 Методические указания для студентов по освоению дисциплины

1. Об информации, информационных технологиях и о защите информации: [Электронный ресурс] : федер. закон от 27 июля 2007 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. О персональных данных : [Электронный ресурс] : федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Козунова, С. С. Системы управления информационной безопасностью предприятия [Электронный ресурс] / С. С. Козунова // Евразийский союз ученых. -2016. - № 28-2. С. 22-23. – Режим доступа: http://elibrary.ru/query_results.asp?pagenum=3.

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1 Электронно-библиотечная система ZNANIUM.COM. Договор ЕП 44 № 003/10 эбс ИКЗ 191272700076927030100100120016311000 от 17 апреля 2019 г.

2 Электронно-библиотечная система IPRbooks. Лицензионный договор № ЕП44 № 001/9 на предоставление доступа к электронно-библиотечной системе IPRbooks ИКЗ 191272700076927030100100090016311000 от 27 марта 2019 г.

3 Электронно-библиотечная система eLIBRARY.RU. Договор № ЕП 44 № 004/13 на оказание услуг доступа к электронным изданиям ИКЗ 912727000769270301001001500163110000 от 15 апреля 2019 г.

4 Информационно-справочные системы «Кодекс»/ «Техэксперт». Соглашение о сотрудничестве № 25/19 от 31 мая 2019 г.

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Защита данных. // Национальный открытый университет «Интуит» [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/courses/13845/1242/lecture/27503 - свободный.

8.6 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 7 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты / условия использования
Microsoft Windows Seven	Лицензионный сертификат № 46243844 от 09.12.2009
OpenOffice	Свободная лицензия, условия использования по ссылке: https://www.openoffice.org/license.html
Microsoft Visual Studio 2008/2010/2012/2013/2017	(в составе лицензии dreamspark)

Intellij IDEA Community Edition	Свободная лицензия

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель может проводить инструктаж по выполнению задания. В инструктаж включается:

· цель и содержание задания;

· сроки выполнения;

· ориентировочный объем работы;

· основные требования к результатам работы и критерии оценки;

· возможные типичные ошибки при выполнении.

Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

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

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 8 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
компьютерные классы ФКТ	Учебные лаборатории «Полигон вычислительной техники» 313(5), 201(5), 202(5)	

10.2 Технические и электронные средства обучения

При проведении занятий используется аудитория, оборудованная проектором (стационарным или переносным) для отображения презентаций. Кроме того, при проведении лекций и практических занятий необходим компьютер с установленным на нем браузером и программным обеспечением для демонстрации презентаций.

Для реализации дисциплины подготовлены следующие презентации:

1 Высшее образование в РФ.

2 Виды учебных занятий, виды контроля занятий.

3 Разработка интеллект-карт.

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами,

создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине
Безопасность веб-приложений

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*ИБАС*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины «Анализ и защита веб-приложений» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
ОПК-4: способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	З(ОПК-4) основных подходов к поиску информации в компьютерных системах, сетях, библиотечных фондах	У(ОПК-4) использовать ЭВМ для поиска информации в компьютерных системах, сетях, библиотечных фонда	Н(ОПК-4) поиска информации в компьютерных системах, сетях, библиотечных фондах
ПК-1: способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	З(ПК-1) методов поиска, изучения систематизации и обобщения информации на иностранном языке	У(ПК-1) осуществлять поиск, изучение, обобщение и систематизацию информации на иностранном языке	Н(ПК-1) работы с научно-технической информацией, нормативными и методическими материалами в сфере профессиональной деятельности на иностранном языке

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
1. Концепции веб-сайтов 2. Инъекции 3. Взлом аутентификации и сеанса 4. Утечка важных данных 5. Внешние XML объекты 6. Нарушение контроля доступа 7. Небезопасная конфигурация 8. Межсайтовый скриптинг (XSS) 9. Небезопасная десериализация 10. Использование компонентов с известными уязвимостями 11. Отсутствие журналирования и мониторинга	ОПК-4, ПК-1	Лабораторная работа	Знает основные подходы к поиску информации в компьютерных системах, сетях, библиотечных фондах Умеет осуществлять поиск, изучение, обобщение и систематизацию информации на иностранном языке Владеет навыками работы с научно-технической информацией, нормативными и методическими материалами в сфере профессиональной деятельности на иностранном языке
	ОПК-4, ПК-1	РГР	Знает основные подходы к поиску информации в компьютерных системах, сетях, библиотечных фондах Умеет осуществлять поиск, изучение, обобщение и систематизацию информации на иностранном языке Владеет навыками работы с научно-технической информацией, нормативными и методическими материалами в сфере профессиональной деятельности на иностранном языке

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Концепции веб-сайтов. Принципы работы веб-серверов и веб-приложений. Принципы безопасности веб-сайтов и веб-приложений. Что такое OWASP. Обзор классификации OWASP Top 10. Знакомство с инструментами для выполнения атак. Настройка лаборатории	2		3	5
Инъекции. Что такое инъекции и почему они становятся возможными. Не SQL инъекции. Простые SQL инъекции. Слепые SQL инъекции	1		3	5
Взлом аутентификации и сеанса. Атаки на аутентификацию. Атаки на управление сеансом	1		3	5
Утечка важных данных. Принципы атак, приводящих к утечке данных	1		3	5
Внешние XML объекты. Что такое внешние объекты XML (XXE). Принципы атак на внешние объекты XML	2		3	5
Нарушение контроля доступа. Концепции DOR. Принципы атак на функциональный уровень. Что такое обход каталога. Предназначение заголовка хоста в HTTP. Концепции подключения локального или удаленного файла. Другие возможности ограничения доступа. Что такое подделка запросов на стороне сервера (SSRF). Что такое внешние объекты XML (XXE)	2		3	5
Небезопасная конфигурация. Принципы атак на конфигурацию. Произвольный доступ к файлам в Samba. Файл междоменной политики Flash. Общие ресурсы в AJAX. Межсайтовая трассировка (XST)	2		3	5
Межсайтовый скриптинг (XSS). Концепции XSS. Отраженные XSS. Что такое JSON. Что такое AJAX. Что такое функция Eval. Что такое атрибут HREF. Что такое phpMyAdmin. Хранимые XSS	2		3	5
Небезопасная десериализация. Что такое сериализация и десериализация. Принципы атак на небезопасную десериализацию	1		3	5

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Использование компонентов с известными уязвимостями. Концепции инвентаризации уязвимостей. Что такое переполнение буфера	1		3	5
Отсутствие журналирования и мониторинга. Концепции журналирования в веб-приложениях	1		2	5
РГР				5
ИТОГО по дисциплине	**16**		**32**	**60**

Задания для текущего контроля

Лабораторные работы (11 штук)

12. Установка, настройка и запуск учебного сайта
13. Выполнение атак на учебный веб-сайт с применением инъекций и защита сайта от таких атак.
14. Выполнение атак на учебный веб-сайт с применением атак на аутентификацию и управление сеансом.
15. Выполнение атак на учебный веб-сайт с применением техник раскрытия чувствительных данных и защита сайта от таких атак.
16. Выполнение XXE атак на учебном веб-сервере и защита.
17. Выполнение атак на функционал учебного веб-сервера и защита.
18. Выполнение атак на конфигурацию учебного веб-сервера и защита от таких атак.
19. Выполнение атак на учебный веб-сайт с помощью отраженных и хранимых XSS и защита сайта от таких атак.
20. Выполнение атак на учебный веб-сайт с уязвимостью небезопасной десериализации и защита сайта от таких атак.
21. Выполнение атак на учебный веб-сервер с использованием эксплойтов на известные уязвимости и защита сервера от таких атак.
22. Изучение концепций и практических примеров отсутствия журналирования и мониторинг.

Примерные темы РГР

4. Провести XXE атаки на учебном веб-сервере и защита.
5. Управление жесткими дисками - системная утилита Paragon Partition Manager
6. Резервное копирование и восстановление данных - системная утилита Paragon Drive Backup Professional

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД