ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.05.02 Безопасность веб-приложений

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины

- формирование у студентов знаний об основных типах атак на web-приложения и методов. Их предотвращения. Знания, получаемые в ходе изучения данной дисциплины, позволят студентам не допускать стандартных ошибок в области безопасности при разработке web-приложений.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность веб-приложений» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Безопасность веб-приложений» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенции	Дисциплина
ОПК-3	Языки программирования Операционные системы Операционная система FreeBSD
ПК-5	Основы информационной безопасности
ПК-10	Теория информации Технологии и методы программирования Электроника и схемотехника Основы радиотехники Операционные системы Операционная система FreeBSD

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенции	Дисциплина
ОПК-3,ПК-5	Производстненная научно-исследовательская работа
ПК-5, ПК-10	Производственная (преддипломная) практика
ОПК-3, ПК-5, ПК-10	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОПК-3 - способностью применять языки,	Этап 1: методы программирования и методы	Этап 1: выбирать необходимые инструментальные	Этап 1: владеть современными средствами

системы и инструментальные средства программирования в профессиональной деятельности	разработки эффективных алгоритмов решения прикладных задач.	средства для разработки программ в различных операционных системах и средах.	разработки программного обеспечения на процедурных языках программирования.
ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Этап 2: современные средства разработки и анализа программного обеспечения на языках высокого уровня.	Этап 2: составлять, тестировать, проводить отладку и оформлять программы на языках высокого уровня, включая объектно-ориентированные.	Этап 2: владеть современными средствами разработки программного обеспечения на объектно-ориентированных языках программирования.
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	Этап 1: основные риски информационной безопасности	Этап 1: рассчитывать риски информационной безопасности	Этап 1: рассчета рисков информационной безопасности
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	Этап 2: основные этапы анализа рисков информационной безопасности	Этап 2: разрабатывать методику анализа рисков информационной безопасности	Этап 2 разработки методики анализа рисков информационной безопасности
ПК-10 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	Этап 1: знать физические структуры и основные типы полупроводниковых приборов, их свойства и характеристики;	Этап 1: уметь работать с современной элементной базой электронной аппаратуры;	Этап 1: владеть навыками чтения и составления принципиальных схем базовых функциональных узлов электронной аппаратуры;
ПК-10 -	Этап 2: знать	Этап 2: уметь	Этап 2: владеть

способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	принципы выбора элементной базы для функциональных узлов электронной аппаратуры с учетом требований эксплуатации и экономической эффективности	осуществлять обоснованный выбор структурных и принципиальных схем электронных устройств	навыками оценки параметров электронных приборов и устройств по комплекту документации

4. Объем дисциплины

Объем дисциплины «Организационное и правовое обеспечение информационной безопасности» составляет 5 зачетных единиц (180 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 6	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	38		38	
2	Лабораторные работы (ЛР)				
3	Практические занятия (ПЗ)	38		38	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		20		20

10	Подготовка к занятиям (ПкЗ)		80		80
11	Промежуточная аттестация	4		4	
12	Наименование вида промежуточной аттестации	х	х	экзамен	
13	Всего	80	100	80	100

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Введение. Терминология, статистика атак на web-ресурсы, публичность web-приложений как один из факторов повышенного внимания злоумышленников к web-ресурсам. Атака «злоупотребление функциональностью»**	**6**	**10**		**10**			**x**		**6**	**20**	**x**	**ОПК-3, ПК-5, ПК-10**
1.1.	**Тема 1** Атаки «грубая сила» и «переполнение буфера»	6	6		6			x		4	10	x	ОПК-3, ПК-5, ПК-10
1.2.	**Тема 2** Атака «отказ в обслуживании»: классификация методов, способы защиты	6	4		4			x		2	10	x	ОПК-3, ПК-5, ПК-10

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
2.	**Раздел 2 Атака «межсайтовый скриптинг»6**	**6**	**10**		**10**			**x**		**4**	**20**	**x**	**ОПК-3, ПК-5, ПК-10**
2.1.	**Тема 3** Атака «инъекция команд в протоколы электронной почты»	6	4		4			x		2	10	x	ОПК-3, ПК-5, ПК-10
2.2.	**Тема 4** Понятие LDAP-репозитория (Lightweight Directory Access Protocol), методы атак на LDAP	6	6		6			x		2	10	x	ОПК-3, ПК-5, ПК-10
3.	**Раздел 3 Атака на web-сервер**	**6**	**10**		**10**			**x**		**6**	**20**	**x**	**ОПК-3, ПК-5, ПК-10**
3.1.	**Тема 5** Общая схема функционирования систем с открытыми ключами. Общая схема функционирования систем с открытыми ключами	6	6		4			x		4	10	x	ОПК-3, ПК-5, ПК-10
3.2.	**Тема 6** Защита паролей на Web-серверах	6	4		6			x		2	10	x	ОПК-3, ПК-5, ПК-10
4.	**Раздел 4 Безопасность адресов**	**6**	**8**		**8**			**x**		**4**	**20**	**x**	**ОПК-3, ПК-5, ПК-10**

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
4.1.	**Тема 7** Проверка web-приложений на защиту	6	4		4			x		2	10	x	ОПК-3, ПК-5, ПК-10
4.2.	**Тема 8** Web защита	6	4		4			x		2	10	x	ОПК-3, ПК-5, ПК-10
5.	**Контактная работа**	**6**	**38**		**38**			**x**				**4**	**x**
6	**Самостоятельная работа**	**6**								**20**	**80**		**x**
7.	**Объем дисциплины в семестре**	**6**	**38**		**38**					**20**	**80**	**4**	**x**
8.	**Всего по дисциплине**	**X**	**38**		**38**					**20**	**80**	**4**	**x**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Введение	**2**
Л-2-3	Атака. Межсайтовый скриптинг	**4**
Л-4	Безопасность адресов	**2**
Л-5-6	Атака «инъекция команд в протоколы электронной почты»	**4**
Л-7	Атака «межсайтовый скриптинг»	**2**
Л-8-9	Атака «злоупотребление функциональностью»	**4**
Л-10	Атака «грубая сила»	**2**
Л-11	Атака "снятие отпечатков пальцев"	**2**
Л-12	Безопасности сайта, проверка сайта на уязвимости	**2**
Л-13	Защита СУБД	**2**
Л-14	Безопасность клиентских приложений	**2**
Л-15	Логические атаки	**2**
Л-16	Анализ защищенности Web-приложений	**2**
Л-17	Базовые сведения о Web-технологиях	**2**
Л-18	Атаки на Web-приложения и их предотвращение	**2**
Л-19	Непроверенные редиректы	**2**
Итого по дисциплине		**38**

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы занятий	Объем, академические часы
ПЗ-1	«Защита сайта от взлома»	**2**
ПЗ -2-3	«Защита реального сайта от атаки»	**4**
ПЗ -4	«Межсайтовый скриптинг»	**2**
ПЗ -5-6	«Атака "снятие отпечатков пальцев"»	**4**
ПЗ -7	«Защита от SQL injection»	**2**
ПЗ -8-9	Защита от Cross Site Scripting (XSS)»	**4**
ПЗ -10	«Использование HTTP».	**2**
ПЗ -11	Предотвращение скачивания пользовательских файлов по прямой ссылке».	**2**
ПЗ -12	«Хранение паролей пользователей»	**2**
ПЗ -13	«Шифрование и обфускация кода»	**2**
ПЗ -14	Тесты на простоту и алгоритмы факторизации	**2**
ПЗ -15	«Защита сайта от взлома»	**2**
ПЗ -16	«Защита реального сайта от атаки»	**2**
ПЗ -17	«Межсайтовый скриптинг»	**2**
ПЗ -18	«Атака "снятие отпечатков пальцев"»	**2**
ПЗ -19	«Защита от SQL injection»	**2**
Итого по дисциплине		**38**

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Атаки «грубая сила» и «переполнение буфера»	Атака «межсайтовый скриптинг». Привести примеры. Способы защиты	4
2.	Атака «отказ в обслуживании»: классификация методов, способы защиты	Атака «отказ в обслуживании». Классификация методов. Меры, применяемые для минимизации успешности данного типа атак.	2
3.	Атака «инъекция команд в протоколы электронной почты»	Проверка на знание разновидностей атак на веб сайты	2
4.	Понятие LDAP-репозитория (Lightweight Directory Access Protocol), методы атак на LDAP	Понятие LDAP.Методы атак.	2
5.	Общая схема функционирования систем с открытыми ключами. Общая схема функционирования систем с открытыми ключами	Схемы открытых ключей.	4
6.	Защита паролей на Web-серверах	Защита паролей на Web-серверах. Проверка целостности	2
7.	Проверка web-приложений на защиту	Проверка с помощью утилит	2
8.	Web защита	Виды атак на веб сайты. Разработка защиты конкретных сайтов	2
Итого по дисциплине			20

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Тузовский А.Ф. Проектирование и разработка web-приложений [Электронный ресурс]: учебное пособие/ Тузовский А.Ф.— Электрон. текстовые данные.— Томск: Томский политехнический университет, 2014.— 219 c.

2. Столбовский Д.Н. Основы разработки Web-приложений на ASP.NET [Электронный ресурс]/ Столбовский Д.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 375 c.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Безопасность IIS/ М.Кобб, М.Джост – М.: Национальный Открытый Университет «ИНТУИТ», 2006 – 678с

2. Межсетевое экранирование: Учебное пособие / О.Р. Лапонина. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007. – 343.

6.3 Методические материалы для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:

- конспект лекций;
- методические материалы по выполнению практических (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие включающее:

- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Open Office

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://fstec.ru/normotvorcheskaya/akty

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

Номер ЛР	Тема практических занятий	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ПЗ-1	«Защита сайта от взлома»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -2-3	«Защита реального сайта	957 – Лаборатория аппаратных средств вычислительной системы;	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows

	от атаки»	943 – Лаборатория технологии, методов программирования и программного обеспечения		XP/7; Интегрированный пакет MS Office Standard;
ПЗ -4	«Межсайтовый скриптинг»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -5-6	«Атака "снятие отпечатков пальцев"»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -7	«Защита от SQL injection»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -8-9	Защита от Cross Site Scripting (XSS)»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -10	«Использование HTTP».	957 – Лаборатория аппаратных средств вычислительной системы;	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows

		943 – Лаборатория технологии, методов программирования и программного обеспечения		XP/7; Интегрированный пакет MS Office Standard;
ПЗ -11	Предотвращение скачивания пользовательских файлов по прямой ссылке».	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -12	«Хранение паролей пользователей»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -13	«Шифрование и обфускация кода»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -14	Тесты на простоту и алгоритмы факторизации	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -15	«Защита сайта от взлома»	957 – Лаборатория аппаратных средств вычислительной системы;	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows

		943 – Лаборатория технологии, методов программирования и программного обеспечения		XP/7; Интегрированный пакет MS Office Standard;
ПЗ -16	«Защита реального сайта от атаки»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -17	«Межсайтовый скриптинг»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -18	«Атака "снятие отпечатков пальцев"»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ПЗ -19	«Защита от SQL injection»	957 – Лаборатория аппаратных средств вычислительной системы; 943 – Лаборатория технологии, методов программирования и программного обеспечения	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): _____ Болотова В.С.