Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 10 от 30 мая 2024 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.ДЭ.05.01 Безопасность Web-приложений

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2024

Содержание (рабочая программа)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Безопасность Web-приложений входит в часть, формируемая участниками образовательных отношений (дисциплина по выбору) блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования, Основы проектной деятельности, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Системы искусственного интеллекта, Облачные технологии и услуги, Технологии защищенного документооборота, Правовая защита информации, Методы и средства защиты информации, Технологии работы в социальных сетях, Встроенные языки программирования, Организация вычислительных процессов

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Проектный практикум, Проектирование информационных систем, Управление информационной безопасностью, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности, Цифровая культура в профессиональной деятельности, Интеллектуальные информационные системы, Современные цифровые технологии управления предприятием

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Безопасность Web-приложений в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-1	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-2	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-4	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	54.15/1.5
Занятия лекционного типа	18/0.5
Лабораторные работы (лабораторный практикум)	36/1
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	35.85/1
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 3

очно-заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 7
Контактная работа, в том числе:	4.15/0.12
Занятия лекционного типа	2/0.06
Лабораторные работы (лабораторный практикум)	2/0.06
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	85.85/2.38
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 3

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Безопасность Web-приложений представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Лаборат. работы	ИКР	ГКР		
1.	Разработка сетевых приложений, web-технологии	8	18	0,075		15	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Технологии обеспечения безопасности web-приложений и методы оптимизации	10	18	0,075		20,85	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	18					
	Итого	**18**	**36**	**0.15**		**35.85**	

очно-заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Лаборат. работы	ИКР	ГКР		
1.	Разработка сетевых приложений, web-технологии	1	1	0,075		40	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Технологии обеспечения безопасности web-приложений и методы оптимизации	1	1	0,075		45,85	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	18					
	Итого	**2**	**2**	0.15		**85.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Разработка сетевых приложений, web-технологии	лекция	HTML, JavaScript, CSS
		лекция	PHP, Node.JS
		лекция	Python, MySQL, основы работы с базами данных
		лекция	jQuery, AJAX, сокеты и сетевые функции
2.	Технологии обеспечения безопасности web-приложений и	лекция	Размещение Web-сайта на сервере
		лекция	Индексация сайта, поисковая оптимизация, конвертация трафика
		лекция	Регламенты и методы разработки

	методы оптимизации		безопасных веб-приложений
		лекция	Основные принципы построения безопасных сайтов, отказоустойчивость систем.
		лекция	Безопасная аутентификация и авторизация. Методы шифрования. SQL-инъекции. XSS-инъекции.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Разработка сетевых приложений, web-технологии	лабораторные работы	Создание серверных сценариев с использованием PHP
		лабораторные работы	Обработка данных на форме, организация файлового ввода-вывода
		лабораторные работы	Организация поддержки базы данных
		лабораторные работы	Составление схем XML-документов
		лабораторные работы	Применение AJAX
		лабораторные работы	Использование библиотеки jQuery
		лабораторные работы	Создание сайта на CMS, администрирование и публикация на бесплатном хостинге
		лабораторные работы	Техническая оптимизация, дополнительные настройки web-приложений
		лабораторные работы	Анализ поведенческих факторов
2.	Технологии обеспечения безопасности web-приложений и методы оптимизации	лабораторные работы	Сбор информации о web-приложении
		лабораторные работы	Тестирование защищенности механизма управления доступом и сессиями
		лабораторные работы	Тестирование на устойчивость к атакам отказа в обслуживании
		лабораторные работы	Поиск уязвимостей к атакам XSS
		лабораторные работы	Поиск уязвимостей к атакам SQL-injection
		лабораторные работы	Создание сценариев атаки и защиты web-приложений
		лабораторные работы	Настройка мониторинга безопасной работы web-приложений
		лабораторные работы	Нагрузочное тестирование web-приложений
		лабораторные работы	Проектирование клиентской и серверной частей модуля безопасности web-приложений

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности

выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Разработка сетевых приложений, web-технологии	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Технологии обеспечения безопасности web-приложений и методы оптимизации	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Гранкин, В. Е. Разработка web-сайтов средствами online конструктора uKit : практикум / В. Е. Гранкин. — Москва : Ай Пи Ар Медиа, 2022. — 78 с. — ISBN 978-5-4497-1464-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/117041.html (Будет открыт в 2025 году)

2. Титов, В. А. Разработка WEB-сайта средствами языка HTML : учебное пособие / В. А. Титов, Г. И. Пещеров. — Москва : Институт мировых цивилизаций, 2018. — 184 с. — ISBN 978-5-9500469-3-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/80643.html

Дополнительная литература

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132

Литература для самостоятельного изучения

1. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие для вузов / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2024. — 219 с. — (Высшее образование). — ISBN 978-5-534-16300-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537106

Полуэктова, Н. Р. Разработка веб-приложений : учебное пособие для вузов / Н. Р. Полуэктова. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 204 с. — (Высшее образование). — ISBN 978-5-534-18645-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/545238

2. 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

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)

2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)

3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)

4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

5.6 Лаборатории и лабораторное оборудование

6. Фонд оценочных средств по дисциплине Безопасность Web-приложений:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное

		знаком « + »
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	+
	Тестирование	+
	Практические задачи	+
	Оценка контрольных работ (для заочной формы обучения)	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Пороговый	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Стандартный (в дополнение к пороговому)	Усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен

Повышенный (в дополнение к пороговому, стандартному)	Определения понятий даются неполные, допускается незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки	Выполняются все операции, последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	В целом владение необходимыми навыками и/или имеет опыт

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств
Пороговый	Усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен
Стандартный (в дополнение к пороговому)	Определения понятий даются неполные, допускается незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки	Выполняются все операции, последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	В целом владение необходимыми навыками и/или имеет опыт
Повышенный (в дополнение к пороговому, стандартному)	Чётко и правильно даются определения, полно раскрывается содержание понятий, верно используется терминология, при этом	Выполняются все операции, последовательность их выполнения достаточно хорошо продумана, действие выполняется в	Владение всеми необходимыми навыками и/или имеет опыт

	ответ самостоятельный, использованы ранее приобретенные знания	целом осознано	

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Пороговый	Усвоено основное содержание, но излагается фрагментарно, не всегда последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	Выполняются не все операции действия, допускаются ошибки в последовательности их выполнения, действие выполняется недостаточно осознанно	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен
Стандартный (в дополнение к пороговому)	Определения понятий даются неполные, допускается незначительные нарушения в последовательности изложения, небольшие неточности при использовании научных категорий, формулировки	Выполняются все операции, последовательность их выполнения соответствует требованиям, но действие выполняется недостаточно осознанно	В целом владение необходимыми навыками и/или имеет опыт
Повышенный (в дополнение к пороговому, стандартному)	Чётко и правильно даются определения, полно раскрывается содержание понятий, верно используется терминология, при этом ответ самостоятельный, использованы ранее приобретенные знания	Выполняются все операции, последовательность их выполнения достаточно хорошо продумана, действие выполняется в целом осознано	Владение всеми необходимыми навыками и/или имеет опыт

6.3. Паспорт оценочных материалов

№	Наименование темы	Контролируемые	Вид контроля/используемые

п/п	(раздела) дисциплины	планируемые результаты обучения в соотношении с результатами обучения по программе	оценочные средства	
			Текущий	Промежуточный
1.	Разработка сетевых приложений, web-технологии	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка докладов; Устный/письменный опрос; Тестирование; Практические задачи; Оценка контрольных работ (для заочной формы обучения).	Зачет
2.	Технологии обеспечения безопасности web-приложений и методы оптимизации	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка докладов; Устный/письменный опрос; Тестирование; Практические задачи; Оценка контрольных работ (для заочной формы обучения).	Зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Разработка сетевых приложений, web-технологии	1. Архитектура клиент-серверных приложений: принципы и реализация. 2. Протоколы передачи данных в веб-приложениях: HTTP, HTTPS, WebSocket. 3. Front-end разработка и безопасность: основные уязвимости и защитные меры. 4. Базы данных в веб-приложениях: безопасность и защита от SQL-инъекций. 5. Разработка мобильных веб-приложений: особенности и безопасность.
Технологии обеспечения безопасности web-приложений и методы оптимизации	6. Основы безопасности веб-приложений: аутентификация, авторизация, аудит безопасности. 7. Защита от веб-уязвимостей: XSS (межсайтовый скриптинг), CSRF (межсайтовая подделка запросов), инъекции команд. 8. Шифрование и защита данных в веб-приложениях: HTTPS, криптографические алгоритмы, хэширование паролей. 9. Противодействие DDoS-атакам: методы обнаружения и защиты. 10. Оптимизация производительности веб-приложений при сохранении безопасности: кэширование, сжатие данных, оптимизация запросов к базе данных.

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Разработка сетевых приложений, web-технологии	1. Что такое протокол HTTP? Какие методы запросов вы знаете? 2. Какие основные уязвимости могут быть связаны с клиент-серверной архитектурой веб-приложений? 3. Что такое XSS (межсайтовый скриптинг) и какие меры можно принять

	для защиты от него? 4. Какие методы обеспечения безопасности можно применить при работе с базами данных в веб-приложениях? 5. Какие основные различия между разработкой веб-приложений и разработкой мобильных веб-приложений?
Технологии обеспечения безопасности web-приложений и методы оптимизации	6. Что такое аутентификация и авторизация в контексте веб-приложений? Как они взаимодействуют между собой? 7. Какие основные типы веб-уязвимостей вы знаете? Приведите примеры их проявления. 8. Что такое шифрование данных и какие методы шифрования используются в веб-приложениях? 9. Какие меры можно применить для защиты от DDoS-атак веб-приложений? 10. Какие оптимизационные методы могут быть использованы для улучшения производительности веб-приложений при сохранении безопасности?

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)
https://lms2.sseu.ru/course/index.php?categoryid=1918

Какое из следующих утверждений о SQL-инъекциях является верным?
a) SQL-инъекции не представляют угрозы для безопасности веб-приложений.
b) SQL-инъекции возникают только в старых версиях баз данных.
c) SQL-инъекции могут позволить злоумышленнику выполнить вредоносный SQL-код.
d) SQL-инъекции могут быть предотвращены только с помощью физической защиты сервера. (правильный ответ)

Что такое XSS-атака?
a) Атака, при которой злоумышленник крадет логин и пароль пользователя.
b) Атака, при которой злоумышленник получает доступ к базе данных веб-приложения.
c) Атака, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу, отображаемую у пользователя.
d) Атака, при которой злоумышленник подменяет IP-адрес сервера веб-приложения. (правильный ответ)

Что такое CSRF-атака?
a) Атака, при которой злоумышленник осуществляет аутентификацию от имени другого пользователя.
b) Атака, при которой злоумышленник отправляет пользователя на фальшивый веб-сайт.
c) Атака, при которой злоумышленник манипулирует запросами, отправляемыми от имени аутентифицированного пользователя.
d) Атака, при которой злоумышленник сканирует порты веб-сервера для поиска уязвимостей. (правильный ответ)

Что такое инъекция кода?
a) Атака, при которой злоумышленник вводит некорректные данные в форму на веб-сайте.
b) Атака, при которой злоумышленник передает вредоносный код веб-приложению, которое его выполняет.
c) Атака, при которой злоумышленник изменяет исходный код веб-приложения.
d) Атака, при которой злоумышленник физически проникает в серверное помещение. (правильный ответ)

Какая техника шифрования обеспечивает защищенную передачу данных между клиентом и сервером?
a) MD5

b) AES
c) Base64
d) SSL/TLS (правильный ответ)

Что такое переполнение буфера (buffer overflow)?
a) Атака, при которой злоумышленник превышает лимит доступной памяти на сервере.
b) Атака, при которой злоумышленник получает доступ к базе данных веб-приложения.
c) Атака, при которой злоумышленник передает вредоносные данные, превышающие размер буфера, вызывая перезапись памяти.
d) Атака, при которой злоумышленник манипулирует HTTP-запросами. (правильный ответ)

Что такое аутентификация на основе двух факторов?
a) Аутентификация, при которой пользователь предоставляет два разных логина для доступа к веб-приложению.
b) Аутентификация, при которой пользователь вводит логин и пароль, а затем вводит уникальный код, полученный на свой мобильный телефон.
c) Аутентификация, при которой пользователь должен предоставить два разных пароля для доступа к веб-приложению.
d) Аутентификация, при которой пользователь должен ответить на два сложных математических вопроса. (правильный ответ)

Что такое DDoS-атака?
a) Атака, при которой злоумышленник вводит некорректные данные в форму на веб-сайте.
b) Атака, при которой злоумышленник манипулирует запросами, отправляемыми от имени аутентифицированного пользователя.
c) Атака, при которой злоумышленник отправляет большое количество запросов на сервер, перегружая его и делая его недоступным для легитимных пользователей. (правильный ответ)
d) Атака, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу, отображаемую у пользователя.

Какую роль играет хэширование паролей в безопасности веб-приложений?
a) Хэширование паролей защищает от SQL-инъекций.
b) Хэширование паролей обеспечивает безопасную передачу данных между клиентом и сервером.
c) Хэширование паролей делает пароли нераспознаваемыми для злоумышленников в случае утечки базы данных.
d) Хэширование паролей защищает от перебора паролей и обеспечивает хранение паролей в зашифрованном виде. (правильный ответ)

Что такое межсайтовый скриптинг (XSS)?
a) Атака, при которой злоумышленник передает вредоносный код веб-приложению, которое его выполняет.
b) Атака, при которой злоумышленник отправляет пользователя на фальшивый веб-сайт.
c) Атака, при которой злоумышленник крадет логин и пароль пользователя.
d) Атака, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу, отображаемую у пользователя. (правильный ответ)

Что такое атака на пакеты в сети (packet sniffing)?
a) Атака, при которой злоумышленник осуществляет аутентификацию от имени другого пользователя.
b) Атака, при которой злоумышленник получает доступ к базе данных веб-приложения.
c) Атака, при которой злоумышленник перехватывает и анализирует сетевой трафик с целью получения конфиденциальной информации. (правильный ответ)
d) Атака, при которой злоумышленник отправляет пользователю вредоносные пакеты данных.

Что такое атака на отказ в обслуживании (DoS)?
a) Атака, при которой злоумышленник вводит некорректные данные в форму на веб-сайте.
b) Атака, при которой злоумышленник отправляет большое количество запросов на сервер,

перегружая его и делая его недоступным для легитимных пользователей. (правильный ответ)
c) Атака, при которой злоумышленник манипулирует HTTP-запросами.
d) Атака, при которой злоумышленник перехватывает и анализирует сетевой трафик с целью получения конфиденциальной информации.

Что такое межсайтовая подделка запроса (CSRF)?
a) Атака, при которой злоумышленник осуществляет аутентификацию от имени другого пользователя.
b) Атака, при которой злоумышленник перехватывает и анализирует сетевой трафик с целью получения конфиденциальной информации.
c) Атака, при которой злоумышленник манипулирует запросами, отправляемыми от имени аутентифицированного пользователя. (правильный ответ)
d) Атака, при которой злоумышленник отправляет пользователя на фальшивый веб-сайт.

Что такое аутентификация?
a) Процесс проверки подлинности идентификационных данных пользователя. (правильный ответ)
b) Процесс шифрования передаваемых данных между клиентом и сервером.
c) Процесс контроля доступа пользователя к конкретным функциям веб-приложения.
d) Процесс сохранения пользовательских данных на сервере в зашифрованном виде.

Что такое привилегированный доступ?
a) Доступ к веб-приложению с использованием привилегированного аккаунта администратора.
b) Доступ к базе данных веб-приложения без авторизации.
c) Доступ к конфиденциальной информации пользователя без его согласия.
d) Доступ к функциям и ресурсам веб-приложения, требующим особых прав и разрешений. (правильный ответ)

Что такое инъекция команд?
a) Атака, при которой злоумышленник вводит некорректные данные в форму на веб-сайте.
b) Атака, при которой злоумышленник передает вредоносный код веб-приложению, которое его выполняет.
c) Атака, при которой злоумышленник осуществляет аутентификацию от имени другого пользователя.
d) Атака, при которой злоумышленник внедряет вредоносные команды для выполнения на сервере. (правильный ответ)

Что такое атака через открытый редирект?
a) Атака, при которой злоумышленник осуществляет перенаправление пользователя на вредоносный веб-сайт.
b) Атака, при которой злоумышленник подделывает идентификаторы сессий пользователей.
c) Атака, при которой злоумышленник использует открытые порты сервера для получения контроля над ним.
d) Атака, при которой злоумышленник использует уязвимость в перенаправлении на веб-сайте для выполнения вредоносных действий. (правильный ответ)

Какое из следующих утверждений о хэшировании паролей является верным?
a) Хэширование паролей является необязательной мерой безопасности веб-приложений.
b) Хэширование паролей позволяет безвозвратно преобразовать пароль в нераспознаваемую строку. (правильный ответ)
c) Хэширование паролей защищает от межсайтового скриптинга.
d) Хэширование паролей обеспечивает безопасную передачу данных между клиентом и сервером.

Что такое атака на перехват сессии (session hijacking)?
a) Атака, при которой злоумышленник осуществляет аутентификацию от имени другого пользователя.
b) Атака, при которой злоумышленник получает доступ к базе данных веб-приложения.
c) Атака, при которой злоумышленник перехватывает и использует сессионные данные

пользователя. (правильный ответ)
d) Атака, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу, отображаемую у пользователя.

Что такое принцип наименьших привилегий (least privilege)?
a) Принцип, согласно которому пользователь должен иметь максимально возможные права и привилегии.
b) Принцип, согласно которому веб-приложение должно предоставлять доступ только к тем функциям и ресурсам, которые необходимы для выполнения задачи. (правильный ответ)
c) Принцип, согласно которому доступ к веб-приложению должен быть предоставлен только аутентифицированным пользователям.
d) Принцип, согласно которому веб-приложение должно хранить только минимально необходимую информацию о пользователях.

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)
https://lms2.sseu.ru/course/index.php?categoryid=1918

Раздел дисциплины	Задачи
Разработка сетевых приложений, web-технологии	1. Создание простого веб-сайта с использованием HTML и CSS. 2. Разработка клиент-серверного приложения с использованием протокола HTTP. 3. Реализация формы входа на веб-сайте с проверкой правильности введенных данных. 4. Разработка механизма аутентификации пользователей на веб-сайте. 5. Создание веб-приложения с использованием JavaScript и AJAX для обновления данных на странице без перезагрузки. 6. Реализация защиты от межсайтового скриптинга (XSS) на веб-сайте. 7. Разработка механизма управления сессиями в веб-приложении. 8. Интеграция базы данных в веб-приложение для хранения пользовательских данных. 9. Разработка RESTful API для взаимодействия с веб-приложением. 10. Оптимизация производительности веб-сайта, включая минимизацию и объединение файлов, кэширование и сжатие данных.
Технологии обеспечения безопасности web-приложений и методы оптимизации	11. Реализация механизма двухфакторной аутентификации в веб-приложении. 12. Анализ и устранение уязвимостей веб-приложения с использованием инструментов сканирования уязвимостей. 13. Настройка SSL-сертификата и обеспечение безопасного соединения с веб-сайтом. 14. Разработка механизма защиты от SQL-инъекций в веб-приложении. 15. Применение методов защиты от подделки межсайтовых запросов (CSRF) в веб-приложении. 16. Аудит безопасности веб-приложения и выявление потенциальных уязвимостей. 17. Разработка механизма резервного копирования и восстановления данных в веб-приложении. 18. Использование инструментов обнаружения и предотвращения атак на веб-приложения, таких как WAF (Web Application Firewall). 19. Разработка механизма логирования и мониторинга безопасности веб-приложения. 20. Оптимизация производительности веб-приложения путем оптимизации запросов к базе данных, кэширования и сжатия данных.

Тематика контрольных работ

Раздел дисциплины	Темы

Разработка сетевых приложений, web-технологии	1. Разработка веб-приложения с использованием HTML, CSS и JavaScript. 2. Создание клиент-серверного веб-приложения с использованием протокола HTTP. 3. Реализация механизма аутентификации и авторизации в веб-приложении. 4. Разработка формы входа с проверкой на безопасность введенных данных. 5. Интеграция базы данных в веб-приложение для хранения пользовательских данных.
Технологии обеспечения безопасности web-приложений и методы оптимизации	6. Анализ уязвимостей веб-приложения и разработка мер по их устранению. 7. Разработка механизма защиты от межсайтового скриптинга (XSS). 8. Создание механизма защиты от SQL-инъекций в веб-приложении. 9. Реализация двухфакторной аутентификации в веб-приложении. 10. Оптимизация производительности веб-приложения путем использования кэширования и сжатия данных.

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Разработка сетевых приложений, web-технологии	1. Что такое протокол HTTP и как он используется в веб-разработке? 2. Расскажите о различиях между HTTP и HTTPS. 3. Какие основные инструменты используются при разработке веб-приложений? 4. Что такое AJAX и как он применяется в веб-разработке? 5. Как реализовать механизм аутентификации пользователей в веб-приложении? 6. Что такое сессия и как она используется в веб-разработке? 7. Расскажите о принципе работы и особенностях баз данных для веб-приложений. 8. Какие инструменты и технологии можно использовать для тестирования безопасности веб-приложений? 9. Что такое кросс-сайтовый скриптинг (XSS) и каким образом можно защититься от него? 10. Какие методы оптимизации производительности можно применить при разработке веб-приложений?
Технологии обеспечения безопасности web-приложений и методы оптимизации	11. Что такое уязвимость SQL-инъекции и как ее предотвратить? 12. Расскажите о механизмах аутентификации и авторизации в веб-приложениях. 13. Что такое защита от межсайтового подделывания запроса (CSRF) и как она реализуется? 14. Какие методы шифрования данных применяются для обеспечения безопасности веб-приложений? 15. Что такое уязвимость к внедрению кода (Code Injection) и как ее предотвратить? 16. Каким образом можно защитить веб-приложение от атаки переполнения буфера (Buffer Overflow)? 17. Расскажите о механизмах обнаружения и предотвращения DDoS-атак. 18. Какие методы оптимизации производительности можно применить для веб-приложений? 19. Что такое кэширование и как оно может быть использовано для оптимизации веб-приложений? 20. Каким образом можно обеспечить безопасность передачи данных между клиентом и сервером в веб-приложении?

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	Критерии оценивания для мероприятий контроля с применением 2-х балльной системы
«зачтено»	ПК-1, ПК-2, ПК-4
«не зачтено»	Результаты обучения не сформированы на пороговом уровне