

Документ подписан простой электронной подписью.
Информация о владельце:

ФИО: Кандрашина Елена Александровна

Должность: Врио ректора ФГАОУ ВО «Самарский государственный экономический университет»

Дата подписания: 11.11.2022 11:13:21

Уникальный программный ключ:

b2fd765521f4c570b8c6e8e502a10b4f1de8ae0d

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 № 9 от 31 мая 2022 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

Содержание (рабочая программа)

Стр.

- 1 Место дисциплины в структуре ОП
- 2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 3 Объем и виды учебной работы
- 4 Содержание дисциплины
- 5 Материально-техническое и учебно-методическое обеспечение дисциплины
- 6 Фонд оценочных средств по дисциплине

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:
	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	108
Зачетные единицы	3

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	108
Зачетные единицы	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	ИКР	ГКР		
			Лаборат. работы				
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	

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	ИКР	ГКР		
			Лаборат. работы				
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, сокет и сетевые функции
2.	Технологии обеспечения безопасности web-	лекция	Размещение Web-сайта на сервере
		лекция	Индексация сайта, поисковая оптимизация, конвертация трафика

	приложений и методы оптимизации	лекция	Регламенты и методы разработки 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. Ю. Родичева Нормативная база и стандарты в области информационной безопасности: учеб. пособие для студ. сред. проф. образования / А.В. Остроух. – 1-е изд. – М.: Издательский центр «Академия», 2015. – 208 с

2. Е.В. Михеева Информационные технологии в профессиональной деятельности: учеб. пособие для студ. сред. проф. образования / Е.В. Михеева. – 12-е изд., стер. – М.: Издательский центр «Академия», 2016. – 384 с

Дополнительная литература

1. И.А. Коноплева, О.А. Хохлова, А.В. Денисов Информационные технологии: учебное пособие / под ред. И.А. Коноплевой. – 2-е изд., перераб. и доп. – М.: Проспект, 2010. – 328с.

Литература для самостоятельного изучения

1. Д.Ю. Усенков Коммуникационные технологии: практикум / Д.Ю. Усенков, О.Б. Богомолова. – М.: БИНОМ. Лаборатория знаний, 2013. – 303 с.: ил

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 или GNU/Linux Ubuntu 22.04
2. Microsoft Office 365/2019/2016 (Word, Excel) или LibreOffice 7.3.3
3. WinDjView
4. СУБД MySQL Community edition
5. Node.JS
6. PHP Storm
7. Python 3.10.5 и выше

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

3. 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, утвержденными Ученым советом ФГАОУ ВО СГЭУ, протокол № 9 от 31.05.2022; 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	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
---	---	---	---

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 ответ самостоятельный,	Выполняются все операции, последовательность их выполнения достаточно хорошо продумана, действие выполняется в целом осознано	Владение всеми необходимыми навыками и/или имеет опыт

	использованы ранее приобретенные знания		
--	---	--	--

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 осознанно	Владение всеми необходимыми навыками и/или имеет опыт

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный

		в соотношении с результатами обучения по программе		
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 практических работ Тестирование	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 практических работ Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Разработка сетевых приложений, web-технологии	Виды уязвимостей web-приложений
	Принципы безопасного использования интернет-ресурсов
Технологии обеспечения безопасности web-приложений и методы оптимизации	Классификация угроз информационной безопасности
	Системы идентификации и аутентификации

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Разработка сетевых приложений, web-технологии	Защищенные протоколы передачи данных, принципы работы и применение
	Виды DDoS атак, обнаружение и отражение
Технологии обеспечения безопасности web-приложений и методы оптимизации	Методы обнаружения, эксплуатации и защиты от уязвимостей типа Injection
	Методы обнаружения, эксплуатации и защиты от уязвимостей типа «Грубая сила», «переполнение буфера» и «злоупотребление функциональностью»

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>

- Кто является основным ответственным за определение уровня классификации информации?
 - Руководитель среднего звена
 - Высшее руководство
 - Владелец
 - Пользователь
- Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - Сотрудники
 - Хакеры
 - Атакующие
 - Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- в) Улучшить контроль за безопасностью этой информации
- г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

- а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- б) Необходимый уровень доступности, целостности и конфиденциальности
- в) Оценить уровень риска и отменить контрмеры
- г) Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- а) Владельцы данных
- б) Пользователи
- в) Администраторы
- г) Руководство

6. Что такое процедура?

- а) Правила использования программного и аппаратного обеспечения в компании
- б) Пошаговая инструкция по выполнению задачи
- в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- г) Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- а) Поддержка высшего руководства
- б) Эффективные защитные меры и методы их внедрения
- в) Актуальные и адекватные политики и процедуры безопасности
- г) Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- б) Когда риски не могут быть приняты во внимание по политическим соображениям
- в) Когда необходимые защитные меры слишком сложны
- г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

- а) Пошаговые инструкции по выполнению задач безопасности
- б) Общие руководящие требования по достижению определенного уровня безопасности
- в) Широкие, высокоуровневые заявления руководства
- г) Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- а) Анализ рисков
- б) Анализ затрат / выгоды
- в) Результаты ALE
- г) Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

- а) Количественно оценить уровень безопасности среды
- б) Оценить возможные потери для каждой контрмеры

- в) Количественно оценить затраты / выгоды
- г) Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это: Варианты ответа:

- а) Среднесрочное планирование
- б) Долгосрочное планирование
- в) Ежедневное планирование
- г) Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

- а) Нечто, приводящее к ущербу от угрозы
- б) Любая потенциальная опасность для информации или систем
- в) Любой недостаток или отсутствие информационной безопасности
- г) Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

- а) Технических и нетехнических методов
- б) Контрмер и защитных механизмов
- в) Физической безопасности и технических средств защиты
- г) Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- а) Внедрение управления механизмами безопасности
- б) Классификацию данных после внедрения механизмов безопасности
- в) Уровень доверия, обеспечиваемый механизмом безопасности
- г) Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

- а) Только военные имеют настоящую безопасность
- б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
- в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
- г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

- а) Угрозы x Риски x Ценность актива
- б) (Угрозы x Ценность актива x Уязвимости) x Риски
- в) $SLE \times Частота = ALE$
- г) (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

- а) Делегирование полномочий
- б) Количественная оценка воздействия потенциальных угроз
- в) Выявление рисков
- г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- а) Поддержка
- б) Выполнение анализа рисков
- в) Определение цели и границ
- г) Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- а) Чтобы убедиться, что проводится справедливая оценка
- б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
- г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)

Раздел дисциплины	Задачи
Разработка сетевых приложений, web-технологии	Обработка данных на форме
	Организация файлового ввода-вывода данных
	Организация поддержки базы данных в PHP
	Разработка Web-приложения с помощью XML
	Проведение общего аудита сайта
	Исследование способов ускорения загрузки сайтов
	Улучшение поведенческих факторов
	Техническая оптимизация, дополнительные настройки
	Мультимедиа для веб-приложений
Технологии обеспечения безопасности web-приложений и методы оптимизации	Применение балансировщиков нагрузки
	Сбор информации о web-приложении
	Тестирование защищенности механизма управления доступом и сессиями
	Тестирование на устойчивость к атакам отказа в обслуживании
	Поиск уязвимости к атакам XSS
	Поиск уязвимости к атакам SQL
	Аудит безопасности веб-приложения
	Поиск и ликвидация уязвимостей сайта
	Обнаружение DDoS атак
	Реализация XML-инъекций
Реализация инъекций HTTP в заголовки	

Тематика контрольных работ

Раздел дисциплины	Темы
Разработка сетевых приложений, web-технологии	Сбор исходных данных для разработки web-приложения
	Разработка документации по эксплуатации web-приложения
Технологии обеспечения безопасности web-приложений и методы оптимизации	Жизненный цикл защиты web-приложения.
	Средства защиты базы данных web-приложения.

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. PHP 2. Формы 3. Cookie. HTTP-заголовки ответа сервера. Сессии

	<p>4. Основы работы с базами данных</p> <p>5. Связь с базами данных MySQL</p> <p>6. Объектно-ориентированное программирование на PHP</p> <p>7. PHP и XML</p> <p>8. Сокеты и сетевые функции</p> <p>9. JavaScript</p> <p>10. jQuery</p> <p>11. AJAX</p> <p>12. JavaScript фреймворки React/Vue*</p> <p>13. PHP фреймворки</p>
Технологии обеспечения безопасности web-приложений и методы оптимизации	<p>14. Проблемы безопасности web-приложений.</p> <p>15. Внутренние и внешние угрозы информационной безопасности web-приложения.</p> <p>16. Технологии безопасной передачи информации в сети Интернет.</p> <p>17. Технологии и средства безопасной разработки web-приложения.</p> <p>18. Технологии и средства безопасного развертывания web-приложения.</p> <p>19. Технологии и средства безопасного использования web-приложения.</p> <p>20. Основы тестирования безопасности web-приложения.</p> <p>21. Разработка клиентской части модуля безопасности web-приложения.</p> <p>22. Разработка серверной части модуля безопасности web-приложения.</p> <p>23. Основные виды Интернет-угроз и методы защиты от них.</p> <p>24. Подсистемы защиты web-порталов от информационных атак.</p> <p>25. Особенности исследования web-приложения на уязвимости.</p> <p>26. Специальное программное обеспечение для мониторинга безопасной работы web-приложений.</p>

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