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.05.02 Безопасность мобильных 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 мобильных 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 мобильных 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	оценивать защищенность автоматизированных систем с помощью типовых программных	навыками защищенности автоматизированных систем с помощью типовых программных средств

	средств	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 мобильных 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 мобильных приложений	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 мобильных приложений	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 мобильных приложений	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 мобильных приложений	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 мобильных приложений	лекция	Мобильные платформы. Архитектура мобильных устройств.
		лекция	Использование сторонних библиотек
		лекция	Форматы обмена данными
		лекция	Клиент-серверное взаимодействие
2.	Технологии обеспечения	лекция	Защита информации. Модели угроз
		лекция	Политики ИБ

	безопасности мобильных приложений	лекция	Функционал мобильных устройств. Сертификация.
		лекция	ОС Android и iOS. Обзор, угрозы, средства защиты.
		лекция	Мобильные браузеры. Уязвимости и средства защиты.

*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 мобильных приложений	лабораторные работы	Подключение и использование сторонних библиотек
		лабораторные работы	Маппинг данных
		лабораторные работы	Динамическое поведение объектов интерфейса
		лабораторные работы	Покрытие приложения тестами
		лабораторные работы	Фреймворк Core Data.
		лабораторные работы	Фреймворки Assets Library и Photos.
		лабораторные работы	Карты и геолокация.
		лабораторные работы	Аудио, видео, акселерометр
		лабораторные работы	Фреймворк Core Animation
2.	Технологии обеспечения безопасности мобильных приложений	лабораторные работы	Шифрование данных
		лабораторные работы	Антивирусные средства
		лабораторные работы	Защита средств синхронизации
		лабораторные работы	Перехват SMS-сообщений
		лабораторные работы	Изучение уязвимостей ОС Android
		лабораторные работы	Изучение уязвимостей ОС iOS
		лабораторные работы	Изучение уязвимостей ОС Ubuntu Touch
		лабораторные работы	Изучение возможностей MDM (Mobile Device Management)
		лабораторные работы	Проектирование защиты при использовании концепции BYOD (Bring Your Own Device)

** 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 мобильных приложений	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Технологии обеспечения безопасности	- подготовка доклада

	мобильных приложений	- 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. Каракеян, В. И. Безопасность жизнедеятельности : учебник и практикум для вузов / В. И. Каракеян, И. М. Никулина. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 335 с. — (Высшее образование). — ISBN 978-5-534-17933-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/535496

Дополнительная литература

1. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие для вузов / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2023. — 218 с. — (Высшее образование). — ISBN 978-5-534-00515-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512113

Литература для самостоятельного изучения

1. Резчиков, Е. А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 639 с. — (Высшее образование). — ISBN 978-5-534-17431-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536471

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 мобильных 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	**Планируемые результаты обучения по дисциплине**

результаты обучения по программе			
	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	оценивать защищенность автоматизированных	навыками защищенности автоматизированных

	систем с помощью типовых программных средств	систем с помощью типовых программных средств	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, 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-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	Выполняются не все операции действия, допускаются ошибки в последовательности их	Владение не всеми необходимыми навыками, имеющийся опыт фрагментарен

	последовательно, определения понятий недостаточно четкие, не используются в качестве доказательства выводы и обобщения из наблюдений, допускаются ошибки в их изложении, неточности в профессиональной	выполнения, действие выполняется недостаточно осознанно	
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

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Разработка мобильных приложений	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 мобильных приложений	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	Зачет

			Оценка контрольных работ (для заочной формы обучения)	

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Разработка мобильных приложений	1. Клиент-серверное взаимодействие мобильных приложений. 2. Особенности использования картографических сервисов и геолокации при разработке мобильных приложений.
Технологии обеспечения безопасности мобильных приложений	3. Решение типовых проблем защиты мобильных устройств в корпоративной среде. 4. Современные тенденции и направления развития методов и средств защиты от мобильных угроз.

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Разработка мобильных приложений	1. Описание цикла разработки мобильных приложений и используемых программных средств. 2. Особенности тестирования мобильных приложений.
Технологии обеспечения безопасности мобильных приложений	3. Классификация и методы оценки угроз информационной безопасности от мобильных устройств. 4. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств.

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

1. Какая из следующих угроз является наиболее распространенной для мобильных приложений?
a) Вредоносные программы, такие как вирусы
b) Подделка данных пользователей
c) Взлом паролей (правильный ответ)
d) Физическая кража мобильного устройства

2. Что такое SSL-сертификат?
a) Устройство для защиты физической безопасности мобильного устройства
b) Программное обеспечение для шифрования данных в мобильном приложении
c) Электронный сертификат, который обеспечивает безопасное соединение между клиентом и сервером (правильный ответ)
d) Инструмент для взлома мобильных приложений

3. Что такое OWASP?
a) Организация, занимающаяся разработкой мобильных приложений
b) Международная ассоциация по стандартизации мобильных приложений
c) Проект, предоставляющий список наиболее распространенных уязвимостей веб-приложений (правильный ответ)
d) Технология шифрования данных в мобильных приложениях

4. Что такое обратная разработка (reverse engineering) мобильного приложения?
a) Процесс разработки мобильного приложения с нуля
b) Процесс изучения и анализа работающего мобильного приложения с целью понимания его

структуры и функциональности (правильный ответ)
c) Процесс внедрения вредоносного кода в мобильное приложение
d) Процесс проверки мобильного приложения на наличие уязвимостей

5. Какая техника обеспечивает защиту от атаки перехвата (man-in-the-middle) в мобильных приложениях?
a) Шифрование данных с помощью SSL/TLS (правильный ответ)
b) Установка физических барьеров для мобильных устройств
c) Блокирование IP-адресов злоумышленников
d) Установка антивирусного программного обеспечения на мобильные устройства

6. Какая из следующих мер является наиболее эффективной для защиты мобильных приложений от вредоносных программ?
a) Установка брандмауэра на мобильное устройство
b) Шифрование данных мобильного приложения
c) Регулярные обновления операционной системы и приложений (правильный ответ)
d) Запрет на загрузку сторонних приложений на мобильное устройство

7. Что такое атака "социальная инженерия" в контексте мобильных приложений?
a) Атака, при которой злоумышленник пытается обмануть пользователей, чтобы получить доступ к их личной информации (правильный ответ)
b) Атака, направленная на взлом паролей мобильных приложений
c) Атака, при которой злоумышленник получает физический доступ к мобильному устройству
d) Атака, при которой злоумышленник получает удаленный доступ к серверу мобильного приложения

8. Какой вид аутентификации является наиболее безопасным для мобильных приложений?
a) Аутентификация по паролю
b) Аутентификация по отпечатку пальца
c) Аутентификация по биометрическим данным, таким как сканирование лица или распознавание голоса (правильный ответ)
d) Аутентификация по SMS-коду

9. Что такое декомпиляция (decompilation) мобильного приложения?
a) Процесс удаления вредоносного кода из мобильного приложения
b) Процесс преобразования скомпилированного мобильного приложения в его исходный код (правильный ответ)
c) Процесс проверки мобильного приложения на уязвимости
d) Процесс шифрования данных мобильного приложения

10. Что такое уязвимость "insecure data storage" в мобильных приложениях?
a) Уязвимость, при которой мобильное приложение хранит конфиденциальные данные пользователя в незашифрованном виде на устройстве (правильный ответ)
b) Уязвимость, вызванная отсутствием обновлений операционной системы на мобильном устройстве
c) Уязвимость, вызванная неправильной конфигурацией брандмауэра на мобильном устройстве
d) Уязвимость, при которой мобильное приложение открывает доступ к базе данных других приложений на устройстве

11. Какая из следующих технологий обеспечивает защиту от атаки перебора паролей в мобильных приложениях?
a) CAPTCHA-проверка
b) Многофакторная аутентификация
c) Блокировка учетной записи после нескольких неудачных попыток ввода пароля (правильный ответ)
d) Шифрование паролей на сервере мобильного приложения

12. Что такое уязвимость "side-channel attack" в контексте мобильных приложений?
a) Уязвимость, при которой злоумышленник получает доступ к боковым каналам связи между мобильным устройством и сервером
b) Уязвимость, вызванная отсутствием шифрования данных в мобильном приложении
c) Уязвимость, при которой злоумышленник использует физические характеристики устройства для получения конфиденциальной информации (правильный ответ)
d) Уязвимость, связанная с подделкой IP-адреса мобильного устройства

13. Что такое "санитарная обработка" (sanitization) в мобильных приложениях?
a) Процесс очистки мобильного устройства от вредоносных программ
b) Процесс проверки мобильного приложения на наличие уязвимостей
c) Процесс удаления конфиденциальной информации из памяти мобильного устройства (правильный ответ)
d) Процесс шифрования данных перед их передачей по сети

14. Что такое "тестирование на проникновение" (penetration testing) мобильного приложения?
a) Процесс проверки мобильного приложения на наличие уязвимостей
b) Процесс проверки мобильного приложения на соответствие требованиям функциональности
c) Процесс симуляции реальной атаки на мобильное приложение для выявления уязвимостей и оценки его безопасности (правильный ответ)
d) Процесс удаления вредоносного кода из мобильного приложения

15. Что такое атака "брутфорс" (brute force) в контексте мобильных приложений?
a) Атака, при которой злоумышленник получает доступ к серверу мобильного приложения
b) Атака, при которой злоумышленник использованит специального программного обеспечения для перебора всех возможных комбинаций паролей с целью получения доступа к мобильному приложению (правильный ответ)
c) Атака, при которой злоумышленник перехватывает сетевой трафик между мобильным устройством и сервером
d) Атака, при которой злоумышленник изменяет данные в мобильном приложении

16. Что такое уязвимость "недостаточная аутентификация" в мобильных приложениях?
a) Уязвимость, вызванная отсутствием шифрования данных в мобильном приложении
b) Уязвимость, при которой мобильное приложение позволяет пользователю аутентифицироваться без достаточных проверок (правильный ответ)
c) Уязвимость, вызванная отсутствием защиты от вирусных программ на мобильном устройстве
d) Уязвимость, связанная с физическим доступом к мобильному устройству

17. Что такое "криптографическая защита" в мобильных приложениях?
a) Процесс очистки мобильного устройства от вредоносных программ
b) Процесс шифрования данных в мобильном приложении для обеспечения их конфиденциальности и целостности (правильный ответ)
c) Процесс удаления конфиденциальной информации из памяти мобильного устройства
d) Процесс проверки мобильного приложения на соответствие требованиям безопасности

18. Что такое "тестирование на стороне клиента" (client-side testing) мобильного приложения?
a) Процесс проверки мобильного приложения на наличие уязвимостей, связанных с клиентской частью (правильный ответ)
b) Процесс проверки мобильного приложения на соответствие требованиям функциональности
c) Процесс удаления вредоносного кода из мобильного приложения
d) Процесс симуляции реальной атаки на мобильное приложение для выявления уязвимостей

19. Что такое "защита от обратной разработки" (anti-reverse engineering) в мобильных приложениях?
a) Процесс проверки мобильного приложения на наличие уязвимостей, вызванных обратной разработкой
b) Процесс шифрования и защиты кода мобильного приложенияот обратной разработки с целью

предотвращения его анализа и модификации (правильный ответ)
c) Процесс удаления вредоносного кода из мобильного приложения
d) Процесс симуляции реальной атаки на мобильное приложение для выявления уязвимостей

20. Что такое "безопасное хранилище" (secure storage) в мобильных приложениях?
a) Место для физического хранения мобильных устройств с целью предотвращения кражи
b) Криптографически защищенное хранилище для хранения конфиденциальных данных мобильного приложения (правильный ответ)
c) Специальное программное обеспечение для удаления вредоносных программ с мобильных устройств
d) Место для хранения резервных копий мобильных приложений

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 мобильных приложений	1. Введение в администрирование системами виртуализации 2. Администрирование систем хранения данных (СХД) 3. Конфигурирование сети 4. Создание пользовательского интерфейса 5. Взаимодействие с базами и источниками данных 6. Мониторинг производительности 7. Создание и настройка кластера виртуализации 8. Добавление поддержки поиска в приложение 9. Взаимодействие с Web 3.0 10. Децентрализованные мобильные приложения
Технологии обеспечения безопасности мобильных приложений	11. Сбор информации о мобильном приложении 12. Тестирование защищенности механизма управления доступом и сессиями 13. Отказоустойчивость и защита данных 14. Регулярное обслуживание кода мобильного приложения 15. Настройка и безопасность виртуальных сетей 16. Настройка брендмауэра 17. Настройка антивируса 18. Резервное копирование и восстановление данных 19. Шифрование пользовательских данных 20. Изучение Linux OpenSSH

Тематика контрольных работ

Раздел дисциплины	Темы
Разработка мобильных приложений	1. Базовые принципы функционирования подсистемы контроля доступа 2. Способы защиты службы DNS
Технологии обеспечения безопасности мобильных приложений	3. Создание плана защиты Web-сервер 4. Принципы безопасности с использованием механизма сертификатов

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Разработка мобильных приложений	1. Способы подключения сторонних библиотек. Возможности CocoaPods. Формирование Podfile. 2. Способы организации локального хранения данных. Использование

	библиотеки FMDB и SQLite. 3. Core Data. Хранение данных. Создание модели данных. Обработка результатирующих множеств. Управление таблицами с использованием NSFetchedResultsController. Понятие MagicalRecord. 4. Основные форматы обмена данными. Структура XML. Структура JSON. 5. Парсинг XML. Парсинг JSON. Создание объектов по данным в формате XML и JSON. Использование библиотеки Mantle для маппинга данных в объекты. 6. Принципы клиент-серверного взаимодействия в контексте разработки мобильных приложений для ОС iOS. Инструменты организации клиент-серверного взаимодействия. Библиотека AFNetworking. Обработка исключений. 7. UIKit Dynamics. UIMotionEffect. Протокол UIDynamicItem. UIDynamicAnimator. UIAttachmentBehavior. 8. Работа с изображениями в приложениях для ОС iOS. Захват изображения с камеры. Выбор изображения из галереи устройства. UIImagePickerController. Загрузка изображения из мобильного iOS-приложения в сеть. 9. Отображение карт в мобильном приложении для ОС iOS. Zoom. Отображение геопозиции пользователя. Отметки и аннотации. Обратное геокодирование. 10. Воспроизведение звука в мобильном приложении для ОС iOS. Воспроизведение локальных аудио-файлов. Воспроизведение аудио-файлов из галереи устройства. Воспроизведение потока аудио из сети. Воспроизведение аудио в режиме онлайн. 11. Воспроизведение видео в мобильном приложении для ОС iOS. Воспроизведение локальных видео-файлов. Воспроизведение видео-файлов из галереи устройства. Воспроизведение потока видео из сети. Воспроизведение видео в режиме онлайн. 12. Способы использования акселерометра в мобильных приложениях для ОС iOS. Классы UIAccelerometer и UIAcceleration. Протокол UIAccelerometerDelegate. 13. Особенности работы с Bluetooth в мобильных приложениях для ОС iOS. Core Bluetooth. Объекты CBCentralManager и CBPeripheral. 14. Core Graphics. Трансформация UIView и CALayer. 15. Автоматизация тестирования мобильных приложений для ОС iOS. Тестирование интерфейсов. Crash reporting. 16. Core Animation. Анимируемые property у CALayer.
Технологии обеспечения безопасности мобильных приложений	17. Безопасность в мобильных приложениях для ОС iOS. 18. Безопасность в мобильных приложениях для ОС Android. 19. Безопасность в мобильных приложениях для ОС Ubuntu Touch. 20. Внутренние и внешние угрозы информационной безопасности web-приложения. 21. Технологии безопасной передачи информации в сети Интернет. 22. Технологии и средства безопасной разработки мобильных приложений. 23. Технологии и средства безопасного использования мобильных приложений. 24. Основы тестирования безопасности мобильных приложений. 25. Основные виды Интернет-угроз и методы защиты от них. 26. Особенности исследования мобильных приложений на уязвимости. 27. Специальное программное обеспечение для мониторинга безопасной работы мобильных приложений.

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