МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
МО ЭВМ
Абрамов Г. В.

27.05.2023г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.06 Безопасность мобильных устройств

Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

02.04.02 Фундаментальная информатика и информационные технологии

2. Профиль подготовки/специализация: Технологии разработки мобильных приложений

3. Квалификация выпускника: Магистр

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: *Математического обеспечения ЭВМ*

6. Составители программы: Лебедев Михаил Викторович

7. Рекомендована: НМС факультета ПММ, протокол №7 от 26.05.2023.

)

8. Учебный год:2024-2025 **Семестр(ы):** 4

9.Цели и задачи учебной дисциплины

Цели *учебной дисциплины:*

- Познакомить студентов с основными принципами безопасности мобильных устройств и их важностью в современном информационном обществе.

- Разработать понимание основных угроз безопасности, с которыми сталкиваются мобильные устройства, такие как вредоносные программы, кража данных, фишинг и другие атаки.

- Ознакомить студентов с уязвимостями операционных систем мобильных устройств (например, Android и iOS) и способами их предотвращения.

Задачи учебной дисциплины:

- Изучение основных принципов и терминологии, связанных с безопасностью мобильных устройств и данных.

- Анализ угроз безопасности мобильных устройств и изучение методов их профилактики и обнаружения.

- Ознакомление с методами аутентификации и авторизации для защиты доступа к мобильным устройствам и приложениям.

- Изучение принципов защиты данных на уровне устройства и приложений, включая шифрование и безопасное хранение паролей.

10. Место учебной дисциплины в структуре ООП: (Дисциплина относится к части, формируемой участниками образовательных отношений, блока Б1. Изучение курса должно базироваться на знании учащимися материала курса «Объектно-ориентированное программирование». Дисциплина является продолжением для изучения курсов «Создание мобильных приложений Android» и «Программирование на платформе Android».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников): ПК-1.1, ПК-5.2, ПК-5.3

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
	Способен выбирать технологии и средства разработки мобильных приложений, определять ключевые сценарии для архитектуры мобильных приложений, разрабатывать новые алгоритмические, методические и технологические решения в сфере разработки мобильных приложений	ПК-5	Проектирует архитектуру, оценивание ПО, применяет в практической деятельности профессиональные стандарты в области информационных технологий. Имеет практический опыт в выборе технологий и средств разработки ПО, определяет цели, предположения и ограничения	Знать: современные языки программирования, особенности жизненного цикла разработки ПО, различные методологии его разработки, а также - место тестирования в данном процессе Уметь:решать прикладные задачи в профессиональной сфере деятельности, владеет пакетами программного обеспечения, операционными системами, определять наиболее значимые критерии качества программного продукта, выделять оптимальный вариант. Владеть: технологиями разработки программного обеспечения с учетом требований к окружению, анализируя риски и вырабатывая планы по выполнению тестирования.
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации результатов исследований	ПК-1.1	Обладает фундаментальными знаниями в области математических и естественных наук, информационно-коммуникационных технологий.	Знать: алгоритмы решения поставленной задачи с учетом имеющихся ресурсов Уметь: формировать основные методы и подходы к проведению научно-исследовательских работ. Владеть: методами решения прикладных задач в профессиональной сфере деятельности.

12. Объем дисциплины в зачетных единицах/час — 3/108.

Форма промежуточной аттестации*: Экзамен*

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			3 семестр
Аудиторные занятия			
в том числе:	лекции		12
	практические		
	лабораторные		48
Самостоятельная работа			48
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации *(экзамен – __час.)*			
Итого:			108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Введение в безопасность мобильных устройств: основные понятия и принципы.	Знакомство с основами безопасности мобильных устройств. Рассматриваются ключевые понятия, такие как конфиденциальность, целостность и доступность данных.	https:// https://edu.vsu.ru Безопасность мобильных приложений edu.vsu.ru Безопасность мобильных приложений
1.2	Угрозы безопасности мобильных устройств: вредоносное программное обеспечение, кража данных, фишинг и другие атаки.	Знакомство с различными угрозами безопасности, с которыми сталкиваются мобильные устройства.	https://edu.vsu.ru Безопасность мобильных приложений
1.3	Операционные системы мобильных устройств и их уязвимости.	Знакомство с основными операционными системами мобильных устройств, такие как Android и iOS,	https://edu.vsu.ru Безопасность мобильных приложений
1.4	Методы обнаружения и предотвращения вредоносных приложений на мобильных устройствах.	Знакомство с методами обнаружения и предотвращения вредоносных приложений на мобильных устройствах.	https://edu.vsu.ru Безопасность мобильных приложений

2. Лабораторные занятия			
3.1	Разработка безопасного мобильного приложения:	Реализация приложения, включающего в себя авторизацию, шифрование, проверка на уязвимости	https://edu.vsu.ru Безопасность мобильных приложений
3.2	Изучение возможностей Charles Proxy	Изучение возможностей Charles Proxy	https://edu.vsu.ru Безопасность мобильных приложений

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
	Введение в безопасность мобильных устройств: основные понятия и принципы.	4		10	10	24
	Угрозы безопасности мобильных устройств: вредоносное программное обеспечение, кража данных, фишинг и другие атаки.	8		16	16	40
	Операционные системы мобильных устройств и их уязвимости.	8		10	10	28
	Методы обнаружения и предотвращения вредоносных приложений на мобильных устройствах.	4		6	6	16
	Итого:	24		42	42	108

14. Методические указания для обучающихся по освоению дисциплины

Указание наиболее сложных разделов, работа с конспектами лекций, презентационным материалом. При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	Здзиарски, Дж. iPHONE. Разработка приложений с открытым кодом [Электронный ресурс] / Дж. Здзиарски. - 2-е изд. - СПб.: БХВ-.петербург, 2009. - 357 с. - Режим доступа: http://znanium.com/bookread2.php?book=48937
	Дарвин Ян Ф Android сборник рецептов: задачи и решения для разработчиков приложений. /Ян Ф. Дарвин. М:Вильямс, 2017.-768 с.

3	*Официальная документация по обеспечению безопасности ОС iOS: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf*

б) дополнительная литература:

№ п/п	Источник
	www.lib.vsu.ru – ЗНБ ВГУ
5	OWASP Mobile Security Project / 29 August 2019, at 08:11: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
6	Официальная документация по обеспечению безопасности ОС Android: *https://developer.android.com/training/articles/security-tips*
7	*https://edu.vsu.ru - Образовательный портал «Электронный университет ВГУ»- Электронный ресурс Безопасность мобильных приложений.*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
	https://owasp.org/

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины: (Моноблок Apple iMac MD093RU/A (14 шт.): процессор Intel Core i5 (2.70 GHz), оперативная память 8 Гб, HDD 1 Тб, видеокарта GeForce GT640M 512Мб, диагональ экрана 21,5"

Компьютер APPLE Mac Pro MD772RU/A Xeon W3565 в составе:

системный блок APPLE: процессор Intel Xeon W3565, оперативная память 8Гб, HDD 2Тб, видеокарта AMD Radeon HD 5770

Коммутатор HP ProCurve Switch 1400-24G

Мультимедиа-проектор BENQ MH535

Доска магнитно-маркерная на стенде (100х150см), 2-сторонняя, BRAUBERG PREMIUM

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Введение в безопасность мобильных устройств: основные понятия и принципы.	ПК-5, ПК-1	ПК-5	Собеседование.
2.	Угрозы безопасности мобильных устройств: вредоносное программное обеспечение, кража данных, фишинг и другие атаки.	ПК-5	ПК-5	Лабораторная работа.
	Операционные системы мобильных устройств и их уязвимости.	ПК-5	ПК-5	Собеседование.
	Методы обнаружения и предотвращения вредоносных приложений на мобильных устройствах.	ПК-5	ПК-5	Лабораторная работа.

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Цель лабораторной работы: Ознакомиться с основными функциями и возможностями прокси-сервера Charles Proxy, а также приобрести практические навыки использования этого инструмента в анализе и отладке сетевого трафика.

Задачи:

1. Установка и настройка Charles Proxy: Установите прокси-сервер Charles Proxy на компьютер и настройте его для перехвата и анализа сетевого трафика между клиентом и сервером.
2. Перехват и анализ HTTP-трафика: Запустите Charles Proxy и настройте ваше устройство или приложение для использования прокси-сервера. Затем перехватите и анализируйте HTTP-трафик, включая запросы и ответы между клиентом и сервером.
3. Инспектирование SSL/TLS-трафика: Настройте Charles Proxy для перехвата и дешифровки SSL/TLS-трафика, позволяющего анализировать зашифрованные соединения между клиентом и сервером.
4. Изменение и повторная отправка запросов: Используя возможности Charles Proxy, измените содержимое запросов, включая параметры, заголовки и тело запроса, а затем повторно отправьте запросы для анализа и тестирования поведения приложений.
5. Фильтрация и маркировка трафика: Настройте фильтры в Charles Proxy для отображения только определенного типа трафика или запросов с определенными параметрами.

Маркируйте и цветовыми кодами выделяйте различные типы запросов для более удобного анализа.

6. Защита и обеспечение безопасности: Изучите возможности Charles Proxy в обеспечении безопасности, такие как блокировка определенных запросов, добавление аутентификации или проверка целостности данных.

Перечень *заданий, тем рефератов, тем презентаций, курсовых, докладов, лабораторных работ требования к представлению портфолио*

Описание технологии проведения

Требования к выполнению заданий (или шкалы и критерии оценивания)

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: Лабораторная работа, тесты с вариантами ответов (ПК-1.1; ПК-5.1; ПК-5.2)

Цель лабораторной работы: Изучение принципов и практических аспектов реализации авторизации в мобильных приложениях, а также приобретение навыков в разработке безопасных механизмов аутентификации и авторизации.

Задачи:

1. Проектирование системы авторизации: Определите требования и проектируйте систему авторизации для мобильного приложения. Рассмотрите различные методы аутентификации, такие как вход с использованием имени пользователя и пароля, OAuth, OpenID Connect и другие.
2. Разработка пользовательского интерфейса: Создайте пользовательский интерфейс мобильного приложения для ввода учетных данных и выполнения процесса авторизации. Обеспечьте удобство использования и безопасность при вводе пароля.
3. Реализация клиентской части: Напишите код клиентской части мобильного приложения для отправки запросов на сервер и обработки ответов. Реализуйте механизмы хранения и передачи токенов аутентификации, таких как JWT (JSON Web Token).
4. Разработка серверной части: Создайте серверную часть приложения, которая будет обрабатывать запросы на авторизацию. Реализуйте проверку учетных данных, генерацию и проверку токенов аутентификации, а также механизмы хранения пользовательских данных.
5. Обработка ошибок и безопасность: Учтите возможные угрозы безопасности, такие как подбор пароля, атаки перебора или фишинг. Реализуйте механизмы для обработки ошибок и защиты от таких атак, например, ограничение числа попыток ввода пароля или использование криптографических методов для хранения и передачи учетных данных.
6. Тестирование и отладка: Проведите тестирование разработанной системы авторизации, включая проверку правильности работы, безопасности и устойчивости к атакам. Используйте отладочные инструменты для идентификации и исправления возможных проблем.

Перечень *заданий, тем рефератов, тем презентаций, курсовых, докладов, требования к представлению портфолио, вопросов к экзамену (зачету) и порядок формирования КИМ*

Пример тестов

1. Что такое "Тестирование черного ящика"?
   Правильный ответ: процедура получения и выбора тестовых случаев на основе анализа спецификации
2. Что такое Авторизация?

Правильный ответ: предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

3. Что такое регрессионное тестирование?
   Правильный ответ: Когда в программном обеспечении вносятся определенные изменения для получения желаемого результата, проводится регрессионное тестирование, чтобы проверить, влияет ли текущая логика на выход и работает ли с программным обеспечением, и по-прежнему выводится желаемый результат.
4. Что такое IPC Binder?
   Правильный ответ: механизм, который позволяет вызывать удаленные объекты как локальные и обмениваться файловыми дескрипторами между процессами.
5. Что такое Аутентификация?
   Правильный ответ: процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.
6. Что такое фишинг?
   Правильный ответ: вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

Описание технологии проведения

Текущая аттестация проводится на занятии одновременно во всей учебной группе в виде теста в электронной образовательной среде «Электронный университет ВГУ», адрес курса — https://edu.vsu.ru/course/ Тест составляется из материалов ФОСа, формируется системой автоматически путём добавления случайных вопросов, количество которых соответствует образцу билета. Большая часть вопросов проверяется автоматически, проверки преподавателем с ручным оцениванием требуют только отдельные вопросы, представленные в форме эссе. Ограничение по времени на каждую попытку — 1час 30 минут, количество попыток — 1, выставление окончательной оценки — по высшему баллу.»

Критерии оценки:

оценка «зачтено» выставляется обучающемуся, если правильный ответ дан не менее чем на 60% вопросов;

оценка «не зачтено» выставляется обучающемуся, если правильный ответ дан менее чем на 60% вопросов.

Задания раздела 20.2 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных знаний по результатам освоения данной дисциплины