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

УТВЕРЖДАЮ

Заведующий кафедрой
Сирота Александр Анатольевич
Кафедра технологий обработки и защиты информации

Сирота А.А.

20.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.04.01 Безопасность мобильных приложений

1. Код и наименование направления подготовки/специальности:

09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализация:

Мобильные приложения и компьютерные игры

3. Квалификация выпускника:

Магистратура

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Иванков Александр Юрьевич, к.ф.-м.н., доцент

7. Рекомендована:

Протокол НМС ФКН №5 от 05.03.24

8. Учебный год: 2024-2025 **Семестр(ы)/Триместр(ы):** 2

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

- *получение базовые знаний в области информационной безопасности, криптографии и стеганографии в интересах защиты данных от несанкционированного доступа и обеспечения конфиденциальности обмена информацией в мобильных системах;*
- *получение профессиональных компетенций в области современных технологий защиты информации при разработке мобильных приложений.*

10. Место учебной дисциплины в структуре ООП:

Входит в блок дисциплины по выбору Б1.В.

Входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, информатики и защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен осуществлять определение первоначальных требований, разработку и тестирование информационных систем	ПК-1.1	Умеет осуществлять определение первоначальных требований, назначать и распределять ресурсы при реализации информационной системы	Уметь: применять практические навыки шифрования конфиденциальной информации, контроля за целостностью информации, решения задач идентификации и аутентификации.
ПК-2	Способен разрабатывать стратегии проектирования, определением целей проектирования, критериев эффективности, ограничений применимости	ПК-2.1	Знает современные технологии управления проектами, управление изменениями, инструменты и методы управления заинтересованными сторонами проекта, современные стандарты информационного взаимодействия систем, основы менеджмента, в том числе менеджмента качества, механизмы бизнес-процессов организации	Владеть: базовые принципы защиты конфиденциальной информации, методы идентификации, аутентификации пользователей мобильной системы, принципы организации скрытых каналов передачи информации.
ПК-3	Способен определять варианты структур	ПК-3.1	Умеет проводить анализ внешнесистемных требований,	Знать: теоретическими и практическими аспектами обеспечения информационной безопасности мобильных приложений.

	программного обеспечения информационных систем (программного средства), необходимые информационные потоки и исследовать варианты структур с использованием моделей различного уровня		возможностей их реализации, определяет концептуальный и функциональный облик системы (программного средства), выявление и анализ известных аналогов	

12. Объем дисциплины в зачетных единицах/час. — 5/180.

Форма промежуточной аттестации Зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 2	№ семестра	…
Аудиторные занятия		56	56		
в том числе:	лекции	16	16		
	практические				
	лабораторные	40	40		
Самостоятельная работа		124	124		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*					
Итого:		180	180		

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 приложений	Введение в безопасность мобильных приложений Ключевые области в обеспечении безопасности мобильных приложений Хранение данных	Создан электронный курс, размещены материалы к лекции.
1.2	Обеспечение безопасности в ОС iOS	Обеспечение безопасности в ОС iOS Корневой сертификат Песочница приложения Раздел пользователя Безопасная последовательность загрузки Шифрование и защита данных Классы защиты данных и защита данных связки ключей Взаимодействие с сервером	Создан электронный курс, размещены материалы к лекции.
1.3	Обеспечение безопасности в ОС Android	Обеспечение безопасности в ОС Android Библиотеки криптографии Root доступ и лаунчеры Биометрия Шифрование и защита дынных	Создан электронный курс, размещены материалы к

		Защита паролей	лекции.
1.4	Безопасность мобильных приложений	Тестирование безопасности мобильных приложений Основные типы атак и эксплойтов Статический и динамический анализ кода	Создан электронный курс, размещены материалы к лекции.
1.5	Авторизация и аутентификация	Авторизация и аутентификация Протоколы HTTP, HTTPS, SSL, TLS, VPN Подходы для обеспечения авторизации и аутентификации Хранение ключей и сессий Генерация случайных последовательностей Взаимодействие с ОС Peer-to-peer соединения Локальное хранение данных Встроенные инструменты для аутентификации и авторизации пользователя Взаимодействие с аппаратным комплексом ОС	Создан электронный курс, размещены материалы к лекции.
2. Практические занятия			
3. Лабораторные занятия			
3.1	Введение в безопасность мобильных приложений	Исследование алгоритма Advanced Encryption Standard	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.
3.2	Обеспечение безопасности в ОС iOS	Реализация клиент-серверного мобильного приложения	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.
3.3	Обеспечение безопасности в ОС Android	Разработка программы для подключения к серверу OAUTH 2.0.	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.
3.4	Безопасность мобильных приложений	1. Разработка программы безопасного хранения ключей 2. Реализация приложения с использованием биометрической аутентификации 3. Моделирование атаки "человек посередине"	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.
3.5	Авторизация и аутентификация	Разработка мобильного клиент- серверного приложения с полной защитой данных пользователя	Создан электронный курс. Размещены индивидуальные задания для выполнения

			лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение в безопасность мобильных приложений	2		4	16	22
2	Обеспечение безопасности в ОС iOS	2		6	22	30
3	Обеспечение безопасности в ОС Android	4		6	22	32
4	Безопасность мобильных приложений	4		18	42	64
5	Авторизация и аутентификация	4		6	22	32
	Итого:	16	0	40	124	180

14. Методические указания для обучающихся по освоению дисциплины:

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;

- методические указания и пособия;

- контрольные задания для закрепления теоретического материала;

- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Программирование для мобильных устройств : учебное пособие : [для студ. 3 и 5 курсов фак. ПММ и магистров 1и 2 курсов специальности 010501 - Приклад. математика и информатика, направлений: 010300 - Фундамент информатика и информ. технологии, 010400 - Приклад. математика и информатика] / С.Ю. Болотова, С.Д. Махортов ; Воронеж. гос. ун-т .— Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013 .— 103 с. : ил.

	<URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m13-158.pdf>.
2	Программирование для мобильных устройств [Электронный ресурс] : учебное пособие : [для студ. старших курсов и магистрантов очной формы фак. ПММ, направлений: 01.03.02 - Приклад. математика и информатика, 02.03.02 - Фундаментальная информатика и информ. технологии]. Ч. 3 / ; Воронеж. гос. ун-т .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-247.pdf>.Специальная литература) .— Библиогр.: с.230-242 .— Предм. указ.: с.243-249.— ISBN 978-5-8114-1238-9.

б) дополнительная литература:

№ п/п	Источник
1	Оффициальная документация по обеспечению безопасности в iOS https://www.apple.com/chde/business/docs/site/iOS_Security_Guide.pdf
2	Оффициальная документация по обеспечению безопасности в ОС Android https://static.googleusercontent.com/media/www.android.com/ru//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf

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

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (https://www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024), ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024), ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025), Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027), ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025).

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Программирование для мобильных устройств : учебное пособие : [для студ. 3 и 5 курсов фак. ПММ и магистров 1и 2 курсов специальности 010501 - Приклад. математика и информатика, направлений: 010300 - Фундамент информатика и информ. технологии, 010400 - Приклад. математика и информатика] / С.Ю. Болотова, С.Д. Махортов ; Воронеж. гос. ун-т .— Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013 .— 103 с. : ил. <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m13-158.pdf>.
2	Программирование для мобильных устройств [Электронный ресурс] : учебное пособие : [для студ. старших курсов и магистрантов очной формы фак. ПММ, направлений: 01.03.02 - Приклад. математика и информатика, 02.03.02 - Фундаментальная информатика и информ. технологии]. Ч. 3 / ; Воронеж. гос. ун-т .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2018 <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m18-247.pdf>.

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

1	ОС Windows v.7, 8, 10	Microsoft (прим. 1)	Все ОП факультета

	Windows Server v. 2008-2019	Microsoft	Информационные системы и технологии, Информационные системы и сетевые технологии, Информационные системы в телекоммуникациях.
	PHP	PHP Group	Все ОП факультета
4	Notepad++	GNU	Все ОП факультета
	PuTTY	MIT	Все ОП факультета
	Android Studio	Google, Apache License 2.0	Информационные системы и технологии (магистры)
	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License	Все ОП факультета
	Notepad++	GNU	Все ОП факультета
	Foxit PDF Reader	корпорация FOXIT SOFTWARE INC., проприетарная бесплатная лицензия	Все ОП факультета

18. Материально-техническое обеспечение дисциплины:

290	Учебная аудитория: персональные компьютеры на базе i7-7800x-4ГГц (12 шт.) и персональные компьютера на базе i5-10400-2.90ГГц (14шт.), мониторы ЖК 27". Лабораторное оборудование искусственного интеллекта: рабочие места – модули АО НПЦ "ЭЛВИС" : процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор МС-USB-JTAG (9 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 290
291	Учебная аудитория: персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 291
292	Учебная аудитория: компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6" FHD Lenovo V155-15API.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 292
293	Учебная аудитория: персональные компьютеры на базе Core i7-11700K-3.6 ГГц, мониторы ЖК 24" (15 шт.), мультимедийный проектор, экран. Лабораторное оборудование компьютерной графики видеоадаптеры GeForce RTX 3070.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 293
295	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 24" (24 шт.), мультимедийный проектор, экран. Лабораторное оборудование информационной безопасности операционных систем и программных средств защиты информации от несанкционированного доступа: учебный стенд «Программные средства защиты информации от несанкционированного доступа».	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 295
297	Учебная аудитория: ноутбуки HP EliteBook на базе Intel Core i5-8250U-3.4 ГГц, мониторы ЖК 24" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 297

381	Учебная аудитория: персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19" (12 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 381
382	Учебная аудитория: персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24" (16 шт.), ТВ панель-флипчарт.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 382
383	Учебная аудитория: персональные компьютеры на базе i7-9700F-3ГГц, мониторы ЖК 27" (16 шт.), мультимедийный проектор, экран. Лабораторное оборудование мобильных приложений и игр: рабочие места - персональные компьютеры на базе Intel i7-9700F, видеоадаптеры nVidia GeForce RTX2070, мониторы ЖК 27" (16 шт.); Системы виртуальной реальности HTC Vive Cosmos (2шт.); Беспроводный маршрутизатор TP-Link Archer C7.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 383
384	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 22" (16 шт.), ТВ панель-флипчарт.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 384
385	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 27" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 385
387	Учебная аудитория: мультимедийный проектор, экран. Персональные компьютеры на базе i5-10400-2,9ГГц, мониторы ЖК 27" (12 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 387
314	Учебная аудитория: персональные компьютеры на базе i3-7100-3,6ГГц, мониторы ЖК 19" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 314
316	Учебная аудитория: персональные компьютеры на базе i5-10400-2.9ГГц, мониторы ЖК 19" (30 шт.), мультимедийный проектор, экран. Лабораторное оборудование безопасности компьютерных сетей: стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ. Учебно-методический комплекс "Безопасность компьютерных сетей" ОАО "ИнфоТеКС".	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316

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.	Разделы 1-5 Введение в безопасность мобильных приложений. Обеспечение	ПК-1	ПК-1.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-7.

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	безопасности в ОС iOS. Обеспечение безопасности в ОС Android. Безопасность мобильных приложений. Авторизация и аутентификация.			
2.	Разделы 1-5 Введение в безопасность мобильных приложений. Обеспечение безопасности в ОС iOS. Обеспечение безопасности в ОС Android. Безопасность мобильных приложений. Авторизация и аутентификация.	ПК-2	ПК-2.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-7.
3.	Разделы 1-5 Введение в безопасность мобильных приложений. Обеспечение безопасности в ОС iOS. Обеспечение безопасности в ОС Android. Безопасность мобильных приложений. Авторизация и аутентификация.	ПК-3	ПК-3.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-7.
Промежуточная аттестация форма контроля – зачет с оценкой				

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2

2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 7 лабораторных заданий, предусматривающих разработку и тестирование криптографических и стеганографических алгоритмов	При успешно выполнении работы осуществляется допуск к контрольной работе, в противном случае обучающийся не допускается к контрольной работе.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Пример задания для выполнения лабораторной работы
Лабораторная работа №2
«Реализация клиент-серверного мобильного приложения»

Цель работы:
Реализация мобильного приложения, выполняющего обмен данными с сервером.
Форма контроля: *отчёт в электронном виде*
Количество отведённых аудиторных часов: *8*
Задание:
Получите у преподавателя вариант задания и напишите код, реализующий заданный алгоритм. Визуализируйте результаты и предоставьте их количественные оценки. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель лабораторной работы.
3. Номер своего варианта.
4. Код, написанный исполнителем.
5. Результаты работы программы.

Примеры контрольных вопросов:

1. Какой протокол используется для обмена данными между клиентской и серверной частями системы?

Пример варианта задания:

Реализовать мобильное приложение на базе Android, которое обменивается данными с сервером. Реализовать сценарии обработки клиентских данных на стороне сервера. Разработать интерфейс клиентского приложения для удобного отображения процесса взаимодействия клиента с сервером.

Описание технологии проведения

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Требования к выполнению заданий (или шкалы и критерии оценивания)

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 20.2.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень вопросов к зачету

№	Содержание
1	Ключевые области в обеспечении безопасности мобильных приложений
2	Корневой сертификат в iOS
3	Песочница приложения в iOS
4	Раздел пользователя в iOS
5	Безопасная последовательность загрузки в iOS
6	Шифрование и защита данных в iOS
7	Классы защиты данных и защита данных связки ключей в iOS
8	Библиотеки криптографии в ОС Android
9	Root доступ и лаунчеры в ОС Android
10	Биометрия в ОС Android
11	Шифрование и защита дынных в ОС Android
12	Защита паролей в ОС Android
13	Тестирование безопасности мобильных приложений
14	Основные типы атак и эксплойтов
15	Статический и динамический анализ кода
16	Авторизация и аутентификация
17	Встроенные инструменты для аутентификации и авторизации пользователя

3++

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2023

Направление подготовки / специальность 09.04.02 Информационные системы и технологии

Дисциплина Б1.В.ДВ.04.01 Безопасность мобильных приложений

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Ключевые области в обеспечении безопасности мобильных приложений.
2. Шифрование и защита дынных в ОС Android.

Преподаватель _____ А.Ю. Иванков

Описание технологии проведения

Для оценивания результатов обучения на зачете используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2. умение проводить обоснование и представление основных теоретических и практических результатов (алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

4. владение навыками программирования и исследования криптографических алгоритмов обработки информации в рамках выполняемых лабораторных заданий;

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций и шкала оценок (зачет с оценкой)

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

20.3 Фонд оценочных средств для проверки остаточных знаний (может быть использован для проведения контроля успеваемости в дистанционном режиме)

Компетенция ПК-1

Вопросы с выбором ответа

1. Выберите обязательные атрибуты мобильного устройства:

а) малые габариты и вес;

б) как минимумом один беспроводной интерфейсом доступа к Сети (мобильной связи или Интернет);

в) не менее одного беспроводного персонального сетевого интерфейса типа Bluetooth или NFC;

г) встроенная (несъемная) память;

д) оснащение системой глобального позиционирования;

е) всё перечисленное.

2. Что из перечисленного не является обязательными атрибутами мобильного устройства?

а) одна или несколько цифровых камер;

б) операционная система, не являющаяся полноценной ОС настольных компьютеров и ноутбуков;

в) возможность установки приложений различными способами

г) поддержка съемных носителей;

д) всё перечисленное.

3. Определение понятия мобильная телекоммуникационная система:

а) совокупность аппаратного и программного обеспечения, соединенного в сеть односторонней мобильной связи, обеспечивающие передачу коротких сообщений из центра системы на миниатюрные абонентские приемники.

б) система информационно-коммуникационных технологий в виде совокупности аппаратно и программно совместимого оборудования, соединенного в единую систему (сеть) с целью передачи, хранения и обработки данных мобильных и иных устройств в пределах заранее определённой территории (зоны покрытия).

в) совокупность аппаратного и программного обеспечения, образующая сеть наземной радиотелефонной подвижной связи, обеспечивающая мобильность абонентов в пределах достаточно большой зоны обслуживания, принципиально ориентированная на ведомственную (корпоративную) мобильную связь.

4. Что из перечисленного соответствует понятию протокол?

а) конечная последовательность действий для решения определённой задачи;

б) фиксированная совокупность приемов практической деятельности, приводящей к заранее определенному результату;

в) набор правил, регулирующий процесс передачи данных между двумя точками сети.

5. Определение понятия мобильное приложение:

а) компонент, устанавливаемый на мобильное устройство, подключающийся к серверу мобильной телесистемы и управляющий пользовательским интерфейсом и бизнес-логикой мобильного устройства.

б) комплекс взаимосвязанных программ для решения определенной проблемы (задачи) массового спроса, подготовленный к реализации как любой вид промышленной продукции;

в) паразитный процесс, который потребляет (истощает) ресурсы системы.

6. Назначение аппаратно-программной платформы для корпоративных мобильных приложений:

а) обеспечение автоматизации процесса проектирования на основе комплекса технических, программных и других средств;

б) обеспечение клиент-серверной среды исполнения и инструментов для разработки мобильных приложений;

в) компьютерная поддержка инженерных расчетов для решения различных инженерных задач.

7. Какими основными свойствами характеризуется информация с точки зрения информационной безопасности?

а) целостность;

б) полнота;

в) доступность;

г) адекватность;

д) конфиденциальность;

е) секретность.

8. Что из перечисленного относится к первому уровню стратегии по смягчению последствий компрометации данных при получении доступа злоумышленника к мобильному устройству?

а) защита конфиденциальных данных путем шифрования локального хранилища самого мобильного устройства;

б) использование дополнительных методов аутентификации, например, доменной;

в) запрет локального хранения конфиденциальных данных.

9. Что из перечисленного относится ко второму уровню стратегии по смягчению последствий компрометации данных при получении доступа злоумышленника к мобильному устройству?

а) защита конфиденциальных данных путем шифрования локального хранилища самого мобильного устройства;

б) использование дополнительных методов аутентификации, например, доменной;

в) запрет локального хранения конфиденциальных данных.

10. Что включают в себя стратегии устранения рисков использования недоверенных мобильных устройств?

а) ограничить или запретить использование личных устройств;

б) запуск корпоративных приложений в изолированных контейнерах;

в) применение сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных;

г) обеспечивать безопасность корпоративного устройства, перед выдачей пользователю;

д) взаимная аутентификации для проверки обоих узлов перед передачей данных.

Вопросы с коротким ответом

1. Какой тип архитектуры предполагает обеспечение приложением расширенной функциональности независимо от центрального сервера?

2. Какой тип архитектуры предполагает перенос приложением всех или большей части задач по обработке информации на сервер?

3. Какой этап жизненного цикла решений по безопасности мобильных устройств включает решение ряда подготовительных задач, таких как определение текущих и будущих потребностей, уточнение требований по производительности и функциональности, а также разработку корпоративных политик безопасности при использовании мобильных устройств?

Вопросы с развернутым ответом

1. Перечислите основные ограничения на работу с мобильным устройством в рамках корпоративных политик безопасности.

Критерии оценивания	Шкала оценок
Перечислены основные компоненты политики безопасности (общие, данные, аутентификация, приложения) и приведены все в рамках каждого компонента.	3 балла
Перечислены основные компоненты политики безопасности (общие, данные, аутентификация, приложения) и приведено хотя бы два ограничения в рамках каждого компонента. Имеются незначительные неточности.	2 балла
Перечислены основные компоненты политики безопасности (общие, данные, аутентификация, приложения) и приведено хотя бы одно ограничение в рамках каждого компонента составляющей. Ответ не содержит грубых ошибок.	1 балл
Перечислены не все компоненты политики безопасности (общие, данные, аутентификация, приложения) или не приведено ограничений по какой-либо составляющей. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

1. Общие политики:

- запрет доступа к отдельным модулям устройства (камере, GPS, Bluetooth, USB, карте памяти);

- запрет доступа к встроенному веб-браузеру, почтовому клиенту, службам установки приложений;

- управление беспроводными интерфейсами (Wi-Fi, Bluetooth);

автоматическое отслеживание устройства, определение и оповещение о нарушениях политик.

2. Передача и хранение данных:

- шифрование передачи данных между мобильным устройством и организацией (VPN);

- надежное шифрование локально хранимых данных;

- привязка карты памяти к конкретным устройствам;

- удаленное очищение устройства после нескольких неудачных попыток аутентификации.

3. Аутентификация пользователей и устройств:

- по паролю;

- доменная аутентификация;

- двухфакторная аутентификация.

4. Приложения:

- черный и белый списки;

- управление установкой обновлений и удалением приложений;

- электронная цифровая подпись;

- корпоративный магазин приложений.

2. DLP-системы, описание, назначение, решаемые задачи.

Критерии оценивания	Шкала оценок
В ответе приведено описание и назначение DLP-систем, перечислены основные и побочные задачи.	3 балла
В ответе приведено описание и назначение DLP-систем, частично перечислены основные и побочные задачи.	2 балла
В ответе кратко приведено описание и назначение DLP-систем, частично перечислены основные задачи. Ответ не содержит грубых	1 балл

ошибок.	
В ответе отсутствует описание и назначение DLP-систем или решаемые ими задачи. Имеются грубые ошибки.	0 баллов

Примерное решение:

Системы защиты данных от утечки (DLP) – программные продукты, предотвращающие утечки конфиденциальной информации организации путём построения защищенного цифрового периметра вокруг организации, анализирующие всю исходящую, а в ряде случаев и входящую информацию. Подобные системы осуществляют мониторинг конфиденциальных данных при различных сценариях использования мобильных устройств. Могут быть использованы как решение по контролю за трафиком, предотвращая утечку конфиденциальной информации и позволяя расследовать инциденты, связанные с неправомерными действиями сотрудников.

Основные задачи:

- контроль интернет трафика: мониторинг и анализ данных, отправляемых за пределы организации через почтовые системы, интернет-ресурсы, системы обмена мгновенными сообщениями;

- контроль других информационных потоков: отслеживание документов, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемых на принтере, отправляемых на мобильные носители через Bluetooth и т.д.

Побочные задачи:

- контроль использования рабочего времени и рабочих ресурсов сотрудниками;

- мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;

- контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.);

- выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность.

Компетенция ПК-2

Вопросы с выбором ответа

11. Что включают в себя стратегии устранения рисков компрометации передаваемых данных при использовании небезопасных сетей?

а) запуск корпоративных приложений в изолированных контейнерах;

б) приложения для контроля состояния устройства;

в) применение сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных;

г) взаимная аутентификации для проверки обоих узлов перед передачей данных;

д) всё перечисленное.

12. Что включают в себя стратегии устранения рисков использования небезопасных приложений?

а) запуск корпоративных приложений в изолированных контейнерах;

б) обеспечивать безопасность корпоративного устройства, перед выдачей пользователю;

в) списки разрешенных или запрещенных приложений;

г) безопасный контейнер изоляции корпоративных данных и приложений от всех прочих;

д) ограничение использования браузера.

13. Что включают в себя стратегии устранения рисков использования небезопасных веб-приложений (через браузер)?

а) ограничение использования браузера;

б) блокировка сервисов соединения с доменными службами;

в) запрет доступа к контенту QR-кодов с любых мобильных устройств, применяемых в служебных целях;

г) приложения для контроля состояния устройства;

д) специальный браузер внутри безопасного контейнера для всех рабочих нужд.

14. Что включают в себя стратегии устранения рисков переноса вредоносного программного кода с одного устройства на другое при подключении корпоративного устройства к личному или облачному хранилищу?

а) отключение служб геолокации;

б) средства выбора устройств, с которыми разрешено синхронизироваться;

в) блокировка сервисов соединения с доменными службами;

г) специальный браузер внутри безопасного контейнера для всех рабочих нужд;

д) применение сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных.

Вопросы с коротким ответом

3. Какой этап жизненного цикла решений по безопасности мобильных устройств предполагает выбор используемых технологий управления мобильными устройствами и разработку решений для их развертывания?

Вопросы с развернутым ответом

DLP-системы, общая структура, принцип работы.

Критерии оценивания	Шкала оценок
В ответе присутствует описание принципа работы и описание основных средств анализа (лингвистического, статистического, формального)	3 балла
В ответе присутствует описание принципа работы и описание основных средств анализа (лингвистического, статистического).	2 балла
В ответе присутствует описание принципа работы. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют описание принципа работы и средста анализа. Имеются грубые ошибки.	0 баллов

Примерное решение:

Системы защиты данных от утечки (DLP) – программные продукты, предотвращающие утечки конфиденциальной информации организации.

Примерная структура:

Принцип работы:

В ядре большинства DLP-решений заложены две технологии: лингвистического анализа и технология, основанная на статистических методах. Также в ядре могут использоваться менее распространенные техники, например, применение меток или формальные методы анализа. Разработчики систем противодействия утечкам дополняют уникальный программный алгоритм системными агентами, механизмами управления инцидентами, парсерами, анализаторами протоколов, перехватчиками и другими инструментами.

Технология лингвистической аналитики включает:

- морфологический анализ – поиск по всем возможным словоформам информации, которую необходимо защитить от утечки;

- семантический анализ – поиск вхождений важной (ключевой) информации в содержимом файла, влияние вхождений на качественные характеристики файла, оценка контекста использования.

Статистические методы анализа:

- документ (текст) делится на фрагменты приемлемой величины, с фрагментов снимается хеш (цифровой отпечаток);

- хеш сравнивается с хешами эталонных фрагментов конфиденциальных документов;

- при совпадении система помечает документ как конфиденциальный и действует в соответствии с политиками безопасности.

Анализа формальных структур:

- обнаружение данных определенного формата для любого документа, например, номера счетов или паспорта.

Компетенция ПК-3

Вопросы с выбором ответа

15. Что включает в себя стратегии устранения рисков загрузки небезопасного контента при сканировании QR-кодов?

а) запрет доступа к контенту QR-кодов с любых мобильных устройств, применяемых в служебных целях;

б) специальный браузер внутри безопасного контейнера для всех рабочих нужд;

в) блокировка сервисов соединения с доменными службами;

г) ограничение использования браузера;

д) взаимная аутентификации для проверки обоих узлов перед передачей данных.

16. Что включает в себя стратегии устранения рисков использования геолокации?

а) ограничить или запретить использование личных устройств;

б) запуск корпоративных приложений в изолированных контейнерах;

в) применение сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных;

г) отключение служб геолокаци;

д) запрет использования служб геолокаци конкретными приложениями.

17. К каким последствиям приводит различное вредоносное ПО?

а) хищение персональных данных;

б) потенциальная практическая возможность обхода аутентификации;

в) получение контроля над устройством или вывод его из строя;

г) искажение процессов обработки информации на устройстве;

д) всё перечисленное.

18. К каким последствиям приводят потенциальные ошибки в прошивке или приложении?

а) хищение персональных данных;

б) потенциальная практическая возможность обхода аутентификации;

в) получение контроля над устройством или вывод его из строя;

г) искажение процессов обработки информации на устройстве;

д) всё перечисленное.

19. Перечислите «бытовые» способы защиты мобильного устройства:

а) PIN/пароль;

б) графический ключ;

в) биометрия;

г) антивирусное ПО;

д) всё перечисленное.

20. Выберите компоненты корпоративной политики безопасности передачи и хранения данных:

а) автоматическое отслеживание устройства, определение и оповещение о нарушениях политик;

б) управление установкой обновлений и удалением приложений;

в) шифрование передачи данных между мобильным устройством и организацией (VPN);

г) надежное шифрование локально хранимых данных;

д) удаленное очищение устройства после нескольких неудачных попыток аутентификации.

Вопросы с коротким ответом

5. Какой зарубежный термин применяется для обозначения пользовательского взлома мобильного устройства с целью нарушения встроенных ограничений безопасности?

Вопросы с развернутым ответом

4. Мобильная телекоммуникационная система. Определение, порядок действий при передаче информации.

Критерии оценивания	Шкала оценок
В ответе приведено определение телекоммуникационной системы и перечислены все действия при передаче информации.	3 балла
В ответе приведено определение телекоммуникационной системы и перечислена большая часть действий при передаче информации. Допускаются незначительные неточности.	2 балла
В ответе приведено определение телекоммуникационной системы и перечислена большая часть действий при передаче информации. Ответ не содержит грубых ошибок.	1 балл
В ответе отсутствует определение телекоммуникационной системы или последовательность действий при передаче информации. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

Мобильная телекоммуникационная система – это система информационно – коммуникационных технологий в виде совокупности аппаратно и программно совместимого оборудования, соединенного в единую систему (сеть) с целью передачи, хранения и обработки данных мобильных и иных устройств в пределах заранее определённой территории (зоны покрытия).

Порядок действий при передаче информации:

1. установка соединения между передающей и принимающей сторонами;
2. расчёт оптимального маршрута передачи данных;

3. первичная обработка передаваемой информации (проверка передачи сообщения именно тому, кому оно адресовано);
4. преобразование скорости передачи устройства в скорость, поддерживаемую линией связи;
5. управление потоком передаваемой информации (трафиком).
6. проверка необходимости повторной передачи.
7. повторение передачи в случае возникновения ошибок.

5. Базовые подходы к управлению мобильными устройствами. Описание подходов к управлению мобильными устройствами при наличии и при отсутствии централизованного решения.

Критерии оценивания	Шкала оценок
Приведено полное описание подходов к управлению мобильными устройствами при наличии и при отсутствии централизованного решения.	3 балла
Приведено частичное описание подходов к управлению мобильными устройствами при наличии и при отсутствии централизованного решения.	2 балла
Кратко перечислены составляющие централизованного управления мобильными устройствами. Ответ не содержит грубых ошибок.	1 балл
Отсутствует описание базовых подходов или перечисление их составляющих. Ответ содержит грубые ошибки.	0 баллов

Примерное решение:

Есть два базовых подхода к управлению мобильными устройствами: использование возможностей сервера обмена сообщениями (часто от того же производителя, что и устройства) или использование стороннего продукта, который разработан для управления несколькими марками устройств. В организации установлен один или несколько серверов, обеспечивающих централизованное управление, а на все мобильные устройства устанавливаются клиенты, которые настраиваются для постоянной работы в фоновом режиме.

Если устройство выдано организацией, клиентское приложение обычно управляет конфигурацией и безопасностью всего устройства. Если устройство принадлежит сотруднику, то клиентское приложение управляет только конфигурацией и безопасностью самого приложения и корпоративных данных. Клиентское приложение и корпоративные данные изолированы от прочих приложений и данных устройства, помогая сохранить конфиденциальность как корпоративных данных, так и личного контента пользователя. Централизованное управление мобильными устройствами может задействовать другие корпоративные службы, такие как доменные службы аутентификации и VPN.

Если в организации отсутствует централизованное решение или некоторые мобильные устройства несовместимы с ним, тогда устройствами приходится управлять вручную.

Мобильные устройства часто не предоставляют возможности строго настроить средства безопасности, как это делают клиентские приложения централизованных устройств. Например, мобильные устройства часто поддерживают только простой пароль для аутентификации и не поддерживают надежного шифрования хранилища. Это потребует приобретения, установки, настройки и поддержки целого перечня сторонних приложений, чтобы компенсировать недостающий функционал. Управление устройством, физически не находящимся в стенах организации, может оказаться невозможным. Можно установить утилиты для удаленного управления устройствами, но это потребует значительно больше сил для ручного обновления ПО и прочей технической поддержки мобильных устройств, находящихся вне офиса.

Организации, намеревающиеся использовать мобильные устройства, должны обдумать достоинства каждого сервиса безопасности и определить, какие именно необходимы для их среды.

Правильные ответы

Номер вопроса	Ответ (буква)
1.	а,б,г
2.	а,г
3.	б
4.	в
5.	а
6.	б
7.	а,в,д
8.	а,в
9.	б
10.	а,г
11.	д
12.	в,г
13.	а,д
14.	б,в

15.	а
16.	г,д
17.	а,в
18.	б,г
19.	д
20.	в,г,д

с коротким ответом

Номер вопроса	Ответ (буква)
1.	толстый клиент
2.	тонкий клиент
3.	инициация
4.	разработка
5.	джейлбрейк/jailbreak