

Донецк 2024

Рабочая программа дисциплины «Анализ безопасности мобильных приложений» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (с изм. и доп.). Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

Доцент  
кафедры радиофизики  
и инфокоммуникационных технологий

 М.В. Бабичева

Рабочая программа утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий  
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой

 В.В. Данилов

СОГЛАСОВАНО:

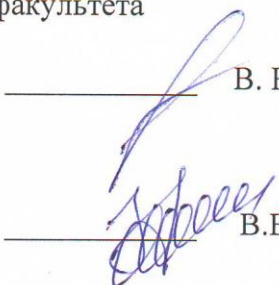
И.о. декана физико-технического факультета  
28.03.2024 г.

 С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета  
Протокол от 27.03.2024 г. № 2  
Председатель

 В. Н. Котенко

Руководитель основной профессиональной  
образовательной программы  
д-р тех. наук, проф.  
26.03.2024 г.

 В.В. Данилов

## 1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

Основы теории сигналов и процессов, Информационные технологии, Технологии и методы программирования.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Системы автоматизированного развертывания приложений, Цифровая обработка сигналов, Современные методы обработки информации.

Используются при написании выпускной квалификационной работы, Производственная практика: научно-исследовательская работа (обязательная). Производственная практика: преддипломная практика (обязательная).

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ

### 2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.4.2 Анализ безопасности мобильных приложений
Часть образовательной программы	Вариативная часть (дисциплины по выбору)
Количество зачетных единиц / всего часов	2,5 / 90

### 2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная, всего	4	8	20	20	-	50	90	зачет

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Формирование фундаментальных знаний основ информатики, форм представления, обработки и передачи информации; изучение технических и программных средств реализации информационных процессов, современных информационных технологий, сетей ЭВМ, методов и средств защиты информации.

## 4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ОПК-3 Способен использовать информационные технологии и	ОПК-3.1. Способен применять программно-аппаратные	Знает основные подходы к защите данных, архитектуру мобильных приложений, внутреннюю структуру мобильной ОС;

программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности.	средства для решения профессиональных задач	Умеет оценивать эффективность защиты данных, искать причины ослабления средств защиты. Владеет навыками оценки надежности алгоритмов и протоколов, методами и практическим применением защиты мобильной ОС.
	ОПК-3.2 Способен применять информационно-коммуникационные технологии для решения профессиональных задач	Умеет строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием средств разработки мобильных приложений на языке программирования Kotlin.

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Установка и настройка окружения.	1.1. Установка Android Studio, создание и настройка эмулятора, подключение физического устройства. 1.2. Основы работы с adb: установка приложения, извлечение приложения. 1.3. Реверс приложения P1 с помощью jadX.
2. Общая информация по платформе андроид.	2.1. Компоненты приложения Андроид. 2.2. Песочница, dex-файлы, id-приложения. 2.3. Активности, Приемники широковебательных намерений. 2.4. Намерения, манифест. Сервисы, поставщики содержимого.
3. Создание приложения Андроид.	3.1. Языки разработки, создание проекта в AS, манифест. 3.2. Элементы управления, дизайн разметки. 3.3. Передача данных между активностями, фрагменты.
4. Безопасность с точки зрения компонентов мобильного приложения.	4.1. Подпись приложения. 4.2. Ресурсы приложения. 4.3. Квалификаторы. 4.4. Обфускация кода.
5. Типовые проверки кода.	5.1. Проверка целостности. 5.2. Проверка на root. 5.3. Проверка на эмуляторе.

6. Приемы работы с инструментами реверса приложений.	6.1. apktools. 6.2. Изменение ресурсов и файлов. 6.3. Основы smali. 6.4. Изменение функциональности, обход проверок.
7. Типовые уязвимости мобильных приложений android.	7.1. Взаимодействие по сети, сниффинг трафика мобильных приложений. 7.2. Способы защиты трафика. SSL-pining. 7.3. Способы “откручивания” ssl-пининга в реальных приложениях.
8. Динамический анализ приложений – frida.	8.1. Основы frida установка и настройка. 8.2. Использование готовых скриптов. frida принципы инъекций, написание собственных скриптов. 8.3. Использование frida для обхода ssl-pining в приложениях, простые и сложные случаи. 8.4. Интеграция frida с python.
9. Objection.	9.2. Работа с окружением, хуки, инъекции в код. 9.3. Дополнительные инструменты анализа и автоматизации.
10. Owasp mobile. организация работ по пен-тесту мобильного приложения.	10.1. mobile top 10 с примерами эксплуатации. 10.2. Создание отчета. 10.3. Программы bug-bounty.

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 4, семестр – 8

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
Установка и настройка окружения.	2	2		5	9
Общая информация по платформе андроид.	2	2		5	9
Создание приложения Андроид.	2	2		5	9
Безопасность с точки зрения компонентов мобильного приложения	2	2		5	9
Типовые проверки кода.	2	2		5	9
Приемы работы с инструментами реверса приложений	2	2		5	9
Типовые уязвимости мобильных приложений android.	2	2		5	9
Динамический анализ приложений – frida.	2	2		5	9
Objection	2	2		5	9
Owasp mobile. Организация работ по пен-тесту мобильного приложения	2	2		5	9
<b>ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП</b>	<b>20</b>	<b>20</b>		<b>47,5+2,5</b>	<b>90</b>
<b>ИТОГО ПО КОМПОНЕНТУ ОПОП</b>	<b>20</b>	<b>20</b>		<b>50</b>	<b>90</b>

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 7.1. Контрольные вопросы

1. Операционные системы для мобильных приложений.
2. Программное обеспечение мобильных приложений.
3. Принципы работы мобильных приложений.
4. Что такое Манифест и какую информацию можно из него получить?
5. Специфика тестирования мобильных приложений: прерывания, пуши, работа с сетью, GPS, ориентация
6. Отличие тестирования мобильных приложений от веб.
7. Системные логи для Android
8. Android Studio для тестирования мобильных приложений.
9. Android Debug Bridge в разработке Android-приложений, основные команды приложения
10. Технологии защиты мобильных приложений.
11. Инструменты для динамического анализа Android-приложений.
12. Инструменты для реверса Android-приложений, jadx
13. Типовые уязвимости мобильных приложений android.
14. Дополнительные инструменты анализа и автоматизации.
15. Owasp mobile, наиболее часто встречающиеся уязвимости в мобильной разработке в 2024 году.
16. Организация работ по пен-тесту мобильного приложения

## 9. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Номера разделов	Виды работ	Максимальное количество баллов
тема 1-17	Текущий контроль	10
	Контрольная работа	20
	Лабораторные работы	40
ИТОГО		70
Зачет		30
Общий итог за семестр		100

### Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

## 10. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа;
  - письменные задания выполняются на компьютере в письменной форме;
  - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;
- 2) для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа.

## 11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в корпусе №4 ДонГУ (г. Донецк, пр. Театральный, 13). Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для проведения лабораторных занятий требуется лаборатория, оснащенная компьютерами с установленным специальным программным обеспечением, указанным в пункте 13.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

## 12. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

### 12.1. Основная литература

1. Искусство тестирования программ / [Сандлер, Майерс, Баджетт]; Диалектика; 2020 г. - 272 с.
2. Основы тестирования программного обеспечения. Учебное пособие / [Старолетов Сергей Михайлович]; Лань; 2022 г. - 382 с.
4. Разработка требований к программному обеспечению. 3-е изд., дополненное / [Вигерс К., Битти Дж.]; БХВ; 2023 г. - 736 с.

### 12.2. Дополнительная литература

5. Тестирование программного обеспечения. Базовый курс/[Святослав Куликов]; ЕРАМ Systems, 2022 г.
6. Что такое тестирование. Курс молодого бойца / [Назина Ольга]; БХВ; 2022г. – 592 с.
7. Эффективное тестирование программного обеспечения / [Маурицио Аниче]; ДМКПресс; 2023 г. - 370 с.

## 13. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Архитектура мобильного клиент-серверного приложения // Хабр, 2023. – URL: <https://habr.com/ru/articles/246877/>
2. Как тестируют мобильные приложения? // Qualitica, 2023. – URL: <https://qualitica.ru/blog/mobile-testing?ysclid=llxhvfkut7353766387>
3. Как установить и пользоваться Android Debug Bridge (ADB) // ROZETKED, 2023. - URL: <https://rozetked.me/articles/21093-kak-ustanovit-i-pol-zovat-sya-android-debugbridge-adb>
4. Коллекция размеров экрана мобильного телефона // URL: <https://www.strerr.com/ru/screen.html>
5. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2023). – Текст : электронный;
6. Учебники и другие книги по математике URL: <http://eqworld.ipmnet.ru/ru/library/mathematics.htm> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный
7. Интернет-библиотека Виталия Арнольда URL: <http://ilib.mccme.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

8. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

9. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный.

#### 14. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Яндекс Браузер (свободно распространяемое ПО)
4. Android Studio — интегрированная среда разработки для работы с платформой Android (свободно распространяемое ПО)
5. Набор инструментов динамического тестирования для разработчиков, специалистов по обратному проектированию и исследователей безопасности Frida (свободно распространяемое ПО)