

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 09:20:01

Уникальный программный ключ:

fd935d10451b860e912264c0378f8448452b603f94388908e29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»**

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»

УТВЕРЖДАЮ

Проректор по учебно-методической работе

 / Г.П. Узунова

«02» февраля 2026 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные мобильные приложения

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника

Бакалавр

Для всех

форм обучения

Симферополь, 2026

Рабочая программа составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» профиль Безопасность компьютерных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 (зарегистрировано в Министерстве юстиции РФ 18.02.2021 №62548) с изменениями и дополнениями.

Программу составил В.Л. Мазниченко, старший преподаватель

Рабочая программа дисциплины «Защищенные мобильные приложения» утверждена на заседании кафедры «Управление и бизнес-информатика».

Протокол № 6 от 29.01.2026 г.

Заведующий кафедрой  Д.В. Моторина
(подпись)

АННОТАЦИЯ	
Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.В.ДВ.03.02	Защищенные мобильные приложения
Цель изучения дисциплины	формирование у студентов профессиональных компетенций, необходимых для разработки мобильных приложений (под платформы Android и iOS), устойчивых к целенаправленным атакам, а также навыков проведения аудита безопасности уже существующих программных продуктов.
Место дисциплины в структуре ОПОП	Дисциплина относится к обязательной части блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-6
Содержание дисциплины	Тема 1. Архитектура защищенности мобильных ОС: модель разрешений и изоляция данных. Тема 2. Безопасное хранение данных на устройстве: Keychain, Keystore и шифрование баз данных. Тема 3. Безопасность транспортного уровня: реализация TLS, Pinning и защита API. Тема 4. Обратная разработка (Reverse Engineering) и обфускация кода. Тема 5. Аутентификация, авторизация и безопасное управление сессиями (Tokens/JWT). Тема 6. Методология тестирования безопасности мобильных приложений (Mobile AppSec).
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)
Форма промежуточной аттестации	Зачет

Содержание

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата	5
2. Место дисциплины в структуре ОПОП бакалавриата	5
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	6
5. Контроль качества освоения дисциплины	11
6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	12
8. Методические указания для обучающихся по освоению дисциплины	13
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	13
10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине	14

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Цель изучения дисциплины «Защищенные мобильные приложения» – формирование у студентов профессиональных компетенций, необходимых для разработки мобильных приложений (под платформы Android и iOS), устойчивых к целенаправленным атакам, а также навыков проведения аудита безопасности уже существующих программных продуктов.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-6	Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.1. Знает формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; ОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Защищенные мобильные приложения относится к обязательной части блока 1. «Дисциплины (модули)» учебного плана ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина «Защищенные мобильные приложения» изучается обучающимися очной формы обучения в 6 семестре, очно-заочной формы обучения – в 6 семестре.

Знания, умения и навыки, полученные при изучении дисциплины «Защищенные мобильные приложения», будут необходимы для углубленного и осмысленного восприятия дисциплин: Системное программирование, Алгоритмизация и программирование и др.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа	38
Аудиторная работа (всего):	38
Лекции	12
Семинары, практические занятия	26
Самостоятельная работа обучающихся (всего)	70
Зачет	+

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 3 зачётных единицы 108 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа	28
Аудиторная работа (всего):	28
Лекции	10
Семинары, практические занятия	18
Самостоятельная работа обучающихся (всего)	80
Зачет	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
		ОФО	ОЗФО	Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Тема 1. Архитектура защищенности мобильных ОС: модель разрешений и изоляция данных.	6	6	2	2	-	-	4	4
2.	Тема 2. Безопасное хранение данных на устройстве: Keychain, Keystore и шифрование баз данных.	12	12	2	2	2	-	8	10
3.	Тема 3. Безопасность транспортного уровня: реализация TLS, Pinning и защита API.	12	12	2	2	2	2	8	8
4.	Тема 4. Обратная разработка	20	20	2	1	14	10	4	9

	(Reverse Engineering) и обфускация кода.								
5.	Тема 5. Аутентификация, авторизация и безопасное управление сессиями (Tokens/JWT).	12	12	2	1	4	4	6	9
6.	Тема 6. Методология тестирования безопасности мобильных приложений (Mobile AppSec).	10	10	2	2	4	4	4	4
	Всего по дисциплине	108	108	12	10	26	18	70	80
	Контроль	-	-						
	Итого	108	108						

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Архитектура защищенности мобильных ОС: модель разрешений и изоляция данных Раскрывается принцип «песочницы» (*sandboxing*): каждое приложение работает в своей изолированной среде с ограниченными правами пользователя *UID*. Изучается система декларативных разрешений (*Permissions*) в Android и App Sandbox в iOS. Рассматриваются риски повышения привилегий, уязвимости экспортируемых компонентов (*ContentProvider*, *BroadcastReceiver*) и механизмы защиты от несанкционированного доступа к файлам одного приложения со стороны другого.

Тема 2. Безопасное хранение данных на устройстве: Keychain, Keystore и шифрование баз данных Изучаются методы локальной защиты информации при наличии физического доступа злоумышленника к смартфону. Рассматривается использование аппаратно-программных модулей (*Secure Enclave* в iOS, *TrustZone/StrongBox* в Android) для хранения ключей. Анализируется практика применения библиотеки *EncryptedSharedPreferences* или *SQLCipher* для шифрования настроек и баз данных вместо хранения их в открытом виде во внутренней памяти.

Тема 3. Безопасность транспортного уровня: реализация TLS, Pinning и защита API Рассматриваются правила безопасного взаимодействия мобильного клиента с серверным бэкендом. Изучается обязательная проверка валидности SSL-сертификатов, механизм закрепления сертификатов (*Certificate Pinning*) для предотвращения атак «человек посередине» (*MitM*) даже при компрометации корневых центров сертификации. Анализируются типичные ошибки реализации сетевых запросов через небезопасные протоколы (*HTTP*, слабые версии *TLS*).

Тема 4. Обратная разработка (Reverse Engineering) и обфускация кода Анализируются угрозы кражи интеллектуальной собственности и извлечения логики работы приложения. Изучается процесс декомпиляции байт-кода (*Smali/Dalvik* для Android, анализ бинарных файлов Mach-O для iOS). Рассматриваются методы противодействия: обфускация имен классов и методов (*ProGuard/R8* для Android), контроль целостности исполняемого файла (*Tamper Detection*) и обнаружение запуска внутри эмулятора или инструментов динамического анализа (*Frida, Objection*).

Тема 5. Аутентификация, авторизация и безопасное управление сессиями (Tokens/JWT) Изучаются современные подходы к проверке подлинности пользователей в мобильных приложениях. Рассматривается безопасный обмен токенами (например, *JWT*),

правила их хранения (избегание незащищенных *SharedPreferences*), механизмы обновления токенов (*Refresh Tokens*) и защита от перехвата сессии. Особое внимание уделяется защите от подделки межсайтовых запросов (*CSRF*) при взаимодействии с веб-интерфейсами внутри приложения.

Тема 6. Методология тестирования безопасности мобильных приложений (Mobile AppSec) Раскрываются инструменты поиска уязвимостей на этапах жизненного цикла разработки (*SDLC*). Изучается статический анализ (*SAST*) исходного кода и бинарных файлов, динамический анализ (*DAST*) запущенного приложения с помощью прокси-инструментов (*Burp Suite, Zap*), а также инструментирование (*IAST*) для отслеживания потока данных (*taint analysis*) в реальном времени. Рассматривается автоматизация проверок с использованием фреймворков (*MobSF, Drozer*).

4.3. Содержание практических занятий (очная форма обучения)

Тема 1. Архитектура защищенности мобильных ОС: модель разрешений и изоляция данных Раскрывается принцип «песочницы» (<i>sandboxing</i>): каждое приложение работает в своей изолированной среде с ограниченными правами пользователя <i>UID</i> . Изучается система декларативных разрешений (<i>Permissions</i>) в Android и App Sandbox в iOS.
Тема 2. Безопасное хранение данных на устройстве: Keychain, Keystore и шифрование баз данных Изучаются методы локальной защиты информации при наличии физического доступа злоумышленника к смартфону. Рассматривается использование аппаратно-программных модулей (<i>Secure Enclave</i> в iOS, <i>TrustZone/StrongBox</i> в Android) для хранения ключей.
Тема 3. Безопасность транспортного уровня: реализация TLS, Pinning и защита API Рассматриваются правила безопасного взаимодействия мобильного клиента с серверным бэкендом. Изучается обязательная проверка валидности SSL-сертификатов, механизм закрепления сертификатов (<i>Certificate Pinning</i>) для предотвращения атак «человек посередине» (<i>MitM</i>) даже при компрометации корневых центров сертификации.
Тема 4. Обратная разработка (Reverse Engineering) и обфускация кода Анализируются угрозы кражи интеллектуальной собственности и извлечения логики работы приложения. Изучается процесс декомпиляции байт-кода (<i>Smali/Dalvik</i> для Android, анализ бинарных файлов Mach-O для iOS).
Тема 5. Аутентификация, авторизация и безопасное управление сессиями (Tokens/JWT) Изучаются современные подходы к проверке подлинности пользователей в мобильных приложениях. Рассматривается безопасный обмен токенами (например, <i>JWT</i>), правила их хранения (избегание незащищенных <i>SharedPreferences</i>), механизмы обновления токенов (<i>Refresh Tokens</i>) и защита от перехвата сессии.
Тема 6. Методология тестирования безопасности мобильных приложений (Mobile AppSec) Раскрываются инструменты поиска уязвимостей на этапах жизненного цикла разработки (<i>SDLC</i>). Изучается статический анализ (<i>SAST</i>) исходного кода и бинарных файлов, динамический анализ (<i>DAST</i>) запущенного приложения с помощью прокси-инструментов (<i>Burp Suite, Zap</i>).

4.4. Содержание самостоятельной работы

Тема 1. Архитектура защищенности мобильных ОС: модель разрешений и изоляция данных

риски повышения привилегий, уязвимости экспортируемых компонентов (ContentProvider, BroadcastReceiver) и механизмы защиты от несанкционированного доступа к файлам одного приложения со стороны другого.
Тема 2. Безопасное хранение данных на устройстве: Keychain, Keystore и шифрование баз данных практика применения библиотеки EncryptedSharedPreferences или SQLCipher для шифрования настроек и баз данных вместо хранения их в открытом виде во внутренней памяти.
Тема 3. Безопасность транспортного уровня: реализация TLS, Pinning и защита API типичные ошибки реализации сетевых запросов через небезопасные протоколы (HTTP, слабые версии TLS).
Тема 4. Обратная разработка (Reverse Engineering) и обфускация кода методы противодействия: обфускация имен классов и методов (ProGuard/R8 для Android), контроль целостности исполняемого файла (Tamper Detection) и обнаружение запуска внутри эмулятора или инструментов динамического анализа (Frida, Objection).
Тема 5. Аутентификация, авторизация и безопасное управление сессиями (Tokens/JWT) защита от подделки межсайтовых запросов (CSRF) при взаимодействии с веб-интерфейсами внутри приложения.
Тема 6. Методология тестирования безопасности мобильных приложений (Mobile AppSec) инструментирование (IAST) для отслеживания потока данных (taint analysis) в реальном времени. Рассматривается автоматизация проверок с использованием фреймворков (MobSF, Drozer).

5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет. Форма проведения промежуточной аттестации – письменный зачет.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

- Осипова, У. В. Разработка мобильных приложений. Программирование мобильных устройств на языке Kotlin : учебное пособие для СПО / У. В. Осипова, И. В. Нечта. — Саратов : Профобразование, 2026. — 78 с. — ISBN 978-5-4488-3046-4. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/161961/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей
- Соколова, В. В. Разработка мобильных приложений : учебное пособие / В. В. Соколова. — 2-е изд. — Москва : Ай Пи Ар Медиа, 2024. — 175 с. — ISBN 978-5-4497-1235-6. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. —

URL: <https://www.iprbookshop.ru/books/147287/details> (дата обращения: 27.01.2026). — Режим доступа: для авторизир. пользователей

б) дополнительная литература:

1. Нужный, А. М. Разработка мобильных приложений : учебное пособие для СПО / А. М. Нужный, Н. И. Гребенникова, В. В. Сафронов. — Саратов : Профобразование, 2022. — 92 с. — ISBN 978-5-4488-1494-5. — Текст : электронный // Образовательная платформа IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/books/121301/details> (дата обращения: 27.01.2026). — DOI: <https://doi.org/10.23682/121301>. — Режим доступа: для авторизир. пользователей

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Информационно-правовой портал «Гарант»: официальный сайт. — URL: <http://www.garant.ru> — Текст: электронный.
2. Цифровой образовательный ресурс «IPRsmart»: официальный сайт. — URL: <http://www.iprbookshop.ru/> — Текст: электронный.
3. Научная электронная библиотека «КиберЛенинка»: официальный сайт. — URL: <https://cyberleninka.ru/> — Текст: электронный.
4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. — URL: <https://www.tadviser.ru/> — Текст: электронный.

8. Методические указания для обучающихся по освоению дисциплины

При проведении лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;
- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижение лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- *программы, обеспечивающие доступ в сеть «Интернет» (например, «Microsoft Edge», «Google Chrome»);
- *программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- *текстовые редакторы и процессоры (например, «Microsoft Office Word»);
- *табличные процессоры (например, «Microsoft Office Excel»);
- *системы управления базами данных (например, «Microsoft Office Access»);
- *программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- *проблемно-ориентированные пакеты прикладных программ по отраслям и сферам деятельности (например, «1С: Управление нашей фирмой», «Loginom Community Edition»).

10. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине

Учебная аудитория

Оборудование учебной аудитории:

рабочее место преподавателя; посадочные места по количеству обучающихся;
доска классная;
стенды информационные.

Учебно-наглядные пособия: ноутбук с лицензионным программным обеспечением и возможностью подключения к информационно-телекоммуникационной сети Интернет; мультимедийная установка; наглядные пособия.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.