Федеральное государственное бюджетное образовательное учреждение высшего образования

**РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА и ГОСУДАРСТВЕННОЙ СЛУЖБЫ при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ**

Факультет среднего профессионального образования

УТВЕРЖДЕНА
решением цикловой (методической) комиссии общепрофессиональных дисциплин и по профессиональным модулям специальности 09.02.07 Информационные системы и программирование
Протокол от 31.10.2025 № 2

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## МДК.03.03 Технологии безопасности мобильных платформ

Специальность – 09.02.11 Разработка и управление программным обеспечением

Профиль – на базе основного общего образования

Квалификация – программист

Форма обучения – очная

Год набора – 2026

Санкт-Петербург 2025 год

**Автор-составитель:** Вилков Владислав Евгеньевич, преподаватель ФСПО СЗИУ РАНХиГС.

**СОДЕРЖАНИЕ**

## 1 Общие положения

### 1.1 Область применения программы

Рабочая программа учебной дисциплины «Технологии безопасности мобильных платформ» является частью основной профессиональной образовательной программы по специальности СПО 09.02.11 «Разработка и управление программным обеспечением».

### 1.2 Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Технологии безопасности мобильных платформ» является частью профессиональной подготовки, входит в общепрофессиональный цикл дисциплин. Базируется на таких дисциплинах, как «Информатика», «Операционные системы и среды», «Основы алгоритмизации и программирования»

Дисциплина изучается на 3 курсе в 6 семестре.

### 1.3 Цели и задачи учебной дисциплины

Цель дисциплины «Технологии безопасности мобильных платформ» — формирование у обучающихся комплексных знаний и практических навыков в области обеспечения информационной безопасности мобильных приложений, включая освоение методов защиты данных, принципов безопасной разработки и противодействия современным угрозам для различных операционных систем.

Задачи дисциплины:

– Сформировать у обучающихся понимание модели угроз для мобильных платформ Android и Aurora, включая изучение распространённых векторов атак и методов их предотвращения

– Развить навыки создания защищённой архитектуры приложения с учётом принципов безопасного хранения данных (EncryptedSharedPreferences, Android Keystore)

– Обучить методам контроля доступа и работы с разрешениями (пермишены и scopes) для обеспечения безопасности пользовательских данных

– Сформировать компетенции в области защиты от распространённых атак: MITM, инжекция кода, подмена Activity

– Развить навыки реализации безопасной аутентификации через изучение принципов работы OAuth2, OpenID и JWT-токенов

– Обучить работе с биометрическими данными (Fingerprint API, Face ID) и их безопасному использованию

– Сформировать понимание принципов безопасной передачи данных через HTTPS и SSL Pinning

– Развить навыки аудита безопасности приложений с использованием инструментов MobSF и OWASP

– Обучить методам защиты от рут-доступа и джейлбрейка

– Сформировать компетенции в области обфускации кода с помощью ProGuard и R8

– Развить навыки применения харденинг-техник (SELinux, AppArmor, Seccomp)

– Обучить работе с политиками безопасности в Aurora и РЕД ОС М

– Сформировать понимание принципов безопасной разработки CI/CD пайплайнов

– Развить навыки проверки соответствия требованиям безопасной разработки

– Сформировать готовность к практическому применению полученных знаний в области защиты мобильных приложений

### 1.4 Планируемые результаты обучения по дисциплине

**Перечень компетенций**

| ***Код ОК, ПК*** | **Уметь** | **Знать** | **Владеть навыками** |
|---|---|---|---|
| ОК.01 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;<br><br>алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач | - |

| | | | |
|---|---|---|---|
| | | профессиональной деятельности | |
| ОК.02 | Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности | номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств | - |
| ОК.03 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях | содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты | - |
| ОК.04 | Эффективно взаимодействовать и | психологические основы деятельности коллектива, | - |

| | | | |
|---|---|---|---|
| | работать в коллективе и команде | психологические особенности личности; основы проектной деятельности | |
| ОК.05 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | особенности социального и культурного контекста; правила оформления документов и построения устных сообщений | - |
| ОК.06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения | - |
| ОК.07 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; принципы бережливого производства; основные направления изменения климатических условий региона | - |

| | | | |
|---|---|---|---|
| ОК.08 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения | - |
| ОК.09 | Пользоваться профессиональной документацией на государственном и иностранном языках | правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности | - |
| ПК 3.1. | − разрабатывать программный код;<br>− отлаживать приложения на различных устройствах;<br>− работать с системами контроля версий;<br>− использовать паттерны проектирования;<br>− осуществлять тестирование кода; | − основы языков программирования;<br>− принципы ООП и функционального программирования;<br>− архитектуры мобильных приложений (MVC, MVVM, VIPER);<br>− принципы работы основных мобильных ОС (iOS, Android); | − разработки модулей программного обеспечения для мобильных платформ;<br>− разработки многопоточных приложений;<br>− оптимизации производительности приложений;<br>работы с интеграцией сторонних библиотек |

| | | | |
|---|---|---|---|
| | − производить рефакторинг; интегрировать приложения с облачными сервисами | − жизненный цикл мобильного приложения;<br>− методы оптимизации производительности;<br>− основы работы с графическим интерфейсом и анимацией;<br>− основы безопасности в мобильной разработке;<br>− основы работы с сетью и API;<br>− принципы работы с базами данных на мобильных платформах; платформы по кроссплатформенной разработке, таких как Flutter, React Native или MAUI. | |
| ПК 3.2. | − создавать интуитивно понятные и легко навигируемые интерфейсы;<br>− использовать анимацию и переходы для улучшения пользовательского опыта;<br>− оптимизировать интерфейс для работы на разных экранах и устройствах;<br>− интегрировать элементы пользовательского интерфейса с серверной частью или базой данных приложения;<br>− анализировать пользовательские данные и обратную связь для улучшения UX;<br>− разрабатывать макеты и прототипы приложений; | − принципы дизайна пользовательского интерфейса (UI) и пользовательского опыта (UX);<br>− основы графического дизайна и типографики;<br>− гайдлайны и стандарты для создания интерфейсов на платформах iOS и Android;<br>− принципы адаптивного дизайна ;<br>− основы работы с векторной и растровой графикой;<br>− процесс проектирования интерфейса от идеи до реализации;<br>− основные принципы дизайна пользовательского интерфейса, таких как иерархия информации, цветовая гамма, типографика и композиция; | − создания пользовательских интерфейсов с использованием инструментов и библиотек, таких как UIKit (iOS) и Android XML (Android);<br>− разработки адаптивных и мультирезолюционных интерфейсов;<br>− тестирования пользовательского опыта;<br>− проведения юзабилити-тестов;<br>− проектирование пользовательского интерфейса (UI) и пользовательского опыта (UX) для различных веб-приложений и сайтов;<br>− разработки прототипов и макетов пользовательского интерфейса с использованием |

| | | | |
|---|---|---|---|
| | − владеть инструментами дизайна интерфейса;<br>− глубоко понимать принципы дизайна пользовательского интерфейса и пользовательского опыта;<br>− проводить пользовательские исследования, включая создание опросов, интервью с пользователями и анализ данных;<br>− работать с прототипированием и созданием макетов пользовательского интерфейса;<br>работать в команде и эффективно взаимодействовать с разработчиками и менеджерами проектов. | − психологию пользователей и их потребности при взаимодействии с веб-приложениями;<br>− современные тенденции в дизайне пользовательского интерфейса и пользовательского опыта;<br>− основные принципы разработки адаптивного и доступного пользовательского интерфейса;<br>основные технологии веб-разработки, такие как HTML, CSS и JavaScript. | инструментов, таких как Sketch, Adobe XD или Figma;<br>− проведения пользовательских исследований, включая сбор обратной связи от пользователей и анализ конкурентного рынка;<br>− создания дизайн-системы и стайл-гайдов для обеспечения единообразия визуального стиля и пользовательского опыта;<br>тестирования и итеративное улучшения пользовательского интерфейса на основе обратной связи пользователей. |
| ПК 3.3. | − проектировать и оптимизировать базы данных;<br>− выполнять CRUD (Create, Read, Update, Delete) операции;<br>− обеспечивать синхронизацию данных между устройствами;<br>− работать с кэшированием данных;<br>− обрабатывать конфликты данных в распределенных системах;<br>− работать с многозадачностью и потоками данных;<br>− владеть языком SQL для работы с базами данных;<br>− глубоко понимать принципы работы с базами данных в | − основы реляционных баз данных;<br>− основы NoSQL и графовых баз данных;<br>− принципы работы с транзакциями;<br>− основы безопасности и шифрования данных;<br>− принципы работы с миграциями баз данных;<br>− основы работы с асинхронными операциями;<br>− основные принципы работы с базами данных в программном обеспечении для мобильных платформ;<br>− различные типы баз данных, таких как реляционные, NoSQL и графовые базы данных;<br>− современные тенденции в разработке | − работы с SQLite и другими СУБД для мобильных платформ;<br>− разработки эффективных схем баз данных;<br>− работы с NoSQL и графовыми базами данных;<br>− работы с ORM (Object-Relational Mapping) инструментами;<br>− работы с асинхронным доступом к данным;<br>− разработки функций и возможностей для работы с базами данных в программном обеспечении для мобильных платформ;<br>− создания интерфейсов для работы с базами |

| | | | |
|---|---|---|---|
| | программном обеспечении для мобильных платформ;<br>− создавать и оптимизировать структуру баз данных для хранения и обработки данных в мобильных приложениях;<br>− работать с ORM (Object-Relational Mapping) инструментами для более удобного взаимодействия с базами данных;<br>обеспечивать безопасность и защиту данных при работе с базами данных в мобильных приложениях. | мобильных приложений с использованием баз данных;<br>− основные принципы проектирования баз данных для эффективного хранения и обработки данных в мобильных приложениях;<br>основные технологии разработки мобильных приложений, таких как Java, Kotlin, Swift или React Native, для работы с базами данных. | данных, включая CRUD операции (создание, чтение, обновление, удаление данных);<br>− интеграции баз данных в пользовательский интерфейс приложений для удобного доступа и управления данными;<br>оптимизации работы с базами данных для обеспечения высокой производительности и эффективного использования ресурсов устройства. |
| ПК 3.4. | − работать с разными форматами изображений и аудиофайлами;<br>− создавать графические ресурсы с высоким разрешением;<br>− проектировать интерфейс с учетом визуальных аспектов, таких как цвета, шрифты и стили;<br>− осуществлять анимацию интерфейсных элементов;<br>− обрабатывать и интегрировать аудио в приложение для воспроизведения звуков и музыки;<br>− владеть инструментами для работы с мультимедиа;<br>− понимать принципы работы с изображениями, видео и аудио в программном | − основы графического дизайна и композиции;<br>− различные форматы изображений и их применение;<br>− основы аудиодизайна и звуковой обработки;<br>− принципы анимации и визуальной привлекательности в мобильных приложениях;<br>− основные принципы работы с изображениями, видео и аудио в программном обеспечении для мобильных платформ;<br>− основные форматы и кодеки для работы с мультимедиа;<br>− современные тенденции в дизайне и использовании мультимедиа в приложениях для мобильных устройств; | − создания и редактирования графических элементов для приложений с использованием специализированных инструментов;<br>− интеграции изображений и иконок в пользовательский интерфейс;<br>− разработки и анимации пользовательских элементов и переходов;<br>− работы с аудиофайлами и интеграции аудио в приложение;<br>− разработки мультимедийных функций и возможностей в программном обеспечении для мобильных платформ; |

| | | | |
|---|---|---|---|
| | обеспечении для мобильных платформ;<br>− создавать и редактировать мультимедийные файлы с использованием различных форматов и кодеков;<br>− работать с анимацией и эффектами для создания привлекательных визуальных элементов в приложениях для мобильных устройств;<br>оптимизировать мультимедийные элементы для обеспечения быстрой загрузки и плавной работы на мобильных устройствах. | − основные принципы разработки мультимедийных функций с учетом ограниченных ресурсов мобильных устройств;<br>основные технологии разработки мобильных приложений, таких как Java, Kotlin, Swift или React Native. | − создания интерфейсов для работы с изображениями, видео и аудио в приложениях для мобильных устройств;<br>− интеграции мультимедийных элементов в пользовательский интерфейс;<br>− оптимизации работы с мультимедиа для обеспечения высокой производительности и эффективного использования ресурсов устройства;<br>получения медиа-данных с помощью механизмов в операционной системе |
| ПК 3.5. | − разрабатывать и запускать тестовые сценарии для проверки функциональности программного обеспечения для мобильных платформ;<br>− выявлять и исправлять ошибки и несоответствия в работе ПО;<br>− проводить аппаратное и программное тестирование программного обеспечения для мобильных платформ;<br>− использовать инструменты анализа и отладки для поиска и устранения проблем;<br>− работать с инструментами для обнаружения и исправления ошибок;<br>− работать с отчетами о тестировании; | − основы тестирования программного обеспечения;<br>− виды тестирования (функциональное, нагрузочное, UI-тестирование и др.);<br>− принципы работы с отладчиками;<br>− основы continuous integration и continuous delivery (CI/CD);<br>− основы создания тестовых сценариев;<br>− принципы и методы тестирования программного обеспечения для мобильных платформ;<br>− особенности отладки программного обеспечения для мобильных платформ;<br>− принципы работы эмуляторов и симуляторов; | − создания тестовых сценариев и единиц тестирования для мобильных платформ;<br>− отладки и анализа проблем в работе мобильных приложений;<br>− использования инструментов и оборудования для тестирования программных компонентов мобильных платформ;<br>работы с эмуляторами и симуляторами для программного обеспечения мобильных платформ |

| | | | |
|---|---|---|---|
| | анализировать и устранять утечки памяти | методы аппаратного и программного тестирования | |
| ПК 3.6. | − проектировать и реализовывать структуру запросов и ответов при работе с API;<br>− аутентифицировать пользователей через сторонние сервисы, такие как OAuth;<br>− обрабатывать и адаптировать данные, получаемые от сторонних сервисов, для использования в приложении;<br>интегрировать функциональность социальных медиа, осуществлять доступ к аппаратным компонентам устройства и управление ими. | − принципы работы с RESTful API и другими протоколами;<br>− основы OAuth и авторизации в сторонних сервисах;<br>стандарты и протоколы взаимодействия с внешними сервисами | − работы с API сторонних сервисов и платформ для получения данных и функциональности;<br>− интеграции социальных медиа и сетей для авторизации и обмена данными;<br>− использования сторонних библиотек и SDK для расширения функциональности приложения;<br>взаимодействия с аппаратными компонентами устройства |
| ПК 3.7. | − разрабатывать и реализовывать меры безопасности;<br>− реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию;<br>− осуществлять валидацию данных, поступающих от пользователей;<br>− разрабатывать политику доступа и права пользователей к данным и функциональности приложения;<br>реализовывать меры контроля доступа и аудита для отслеживания действий пользователей и | − основные угрозы безопасности мобильных приложений;<br>− принципы криптографии и шифрования данных;<br>− стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;<br>− законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;<br>− основные принципы безопасности информации и методов ее защиты;<br>− стандартные криптографические алгоритмы для шифрования данных; | − разработки безопасных методов аутентификации и авторизации пользователей;<br>− обработки и хранения конфиденциальных данных;<br>− отслеживания и обработки уязвимостей безопасности;<br>− использования шифрования для защиты данных в покое и в движении;<br>− использования шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные; |

| | | | |
|---|---|---|---|
| | обнаружения несанкционированных действий. | − методы аутентификации и авторизации пользователей, таких как OAuth или JWT;<br>− многоуровневые механизмы контроля доступа к данным;<br>− методы тестирования на уязвимости безопасности и опыт применения инструментов для их обнаружения;<br>− принципы обеспечения безопасности передачи данных по сети; законодательство и регуляции в области защиты данных и умение применять их в практической разработке мобильных приложений. | − реализации механизмов аутентификации и авторизации для обеспечения доступа только авторизованным пользователям;<br>− применения механизмов хеширования для защиты паролей пользователей от несанкционированного доступа;<br>− обеспечения безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS;<br>− разработки механизмов контроля доступа к данным, чтобы предотвратить несанкционированное чтение, изменение или удаление данных;<br>− проектирования и реализации систем резервного копирования и восстановления данных для обеспечения их сохранности в случае сбоев или потери устройства;<br>− тестирования приложений на уязвимости безопасности, такие как SQL-инъекции, межсайтовые сценарии и другие уязвимости, и принятие мер по их устранению; соблюдение законодательства и |

| | | | |
|---|---|---|---|
| | | | регуляций в области защиты данных |

В результате освоения учебной дисциплины студент должен:

| | |
|---|---|
| иметь практический опыт | – настройки защищённого хранилища данных (EncryptedSharedPreferences, Android Keystore)<br>– проведения аудита безопасности приложений с помощью MobSF<br>– защиты от подмены интентов и MITM-атак<br>– реализации безопасной аутентификации через OAuth2 и OpenID<br>– работы с биометрическими данными (Fingerprint API, Face ID)<br>– настройки SSL Pinning для безопасной передачи данных<br>– проверки устройства на рут/джейлбрейк<br>– применения обфускации кода через ProGuard и R8<br>– реализации политик безопасности в Aurora и РЕД ОС М<br>– настройки харденинг-техник (SELinux, AppArmor, Seccomp)<br>– защиты файлов и кэша во внутреннем и внешнем хранилище<br>– работы с токенами и их валидации<br>– обработки 401/403 ответов и авто-логаута<br>– проверки безопасности межприложенного взаимодействия<br>– внедрения политик безопасности CI/CD |
| уметь | – настраивать безопасное хранение данных<br>– проводить анализ уязвимостей приложения<br>– защищать приложение от распространённых атак<br>– реализовывать безопасную аутентификацию<br>– работать с биометрическими данными<br>– обеспечивать защищённую передачу данных<br>– проверять статус безопасности устройства<br>– применять методы обфускации кода<br>– настраивать политики безопасности<br>– реализовывать защиту данных в хранилище<br>– работать с системой токенов<br>– обрабатывать ошибки аутентификации<br>– обеспечивать безопасность межприложенного взаимодействия<br>– внедрять политики безопасной разработки |
| знать | – модели угроз для Android и Aurora<br>– принципы защищённой архитектуры приложения<br>– механизмы безопасного хранения данных<br>– методы контроля доступа и разрешений<br>– принципы работы распространённых атак<br>– механизмы безопасной аутентификации<br>– принципы работы с биометрическими данными<br>– методы защищённой передачи данных<br>– способы проверки безопасности устройства<br>– методы обфускации кода<br>– принципы работы харденинг-техник<br>– механизмы защиты данных в хранилище<br>– принципы работы с токенами<br>– методы обработки ошибок аутентификации<br>– принципы безопасного межприложенного взаимодействия<br>– требования безопасной разработки CI/CD |

## 2 Структура и содержание дисциплины

### 2.1 Объем учебной дисциплины и виды работ

| Виды учебной работы | Объем учебной работы, час. |
|---|---|
| Учебная нагрузка обучающихся всего, в том числе: | 64 |
| лекции | 22 |
| практические занятия | 40 |
| курсовая работа | - |
| самостоятельная работа обучающихся | - |
| консультации | 2 |
| промежуточная аттестация | - |
| Форма промежуточной аттестации | Зачет с оценкой |

### 2.2 Тематический план и содержание дисциплины

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) | Распределение часов | | | Формируемые компетенции | Формы текущего контроля |
|---|---|---|---|---|---|---|---|
| | | | Л | ПР | СРС | | |
| | **Раздел 1. РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ МОБИЛЬНЫХ ПЛАТФОРМ** | | | | | | |
| 1 | Тема 1.1. Угрозы и модели безопасности | **Содержание учебного материала**<br>Модель угроз Android и Aurora<br>Принципы защищённой архитектуры приложения<br>Secure Storage: EncryptedSharedPreferences, Android Keystore<br>Контроль доступа: пермишены и scopes<br>Распространённые атаки: MITM, инжекция, подмена Activity<br>Особенности защиты в РЕД ОС М<br>В том числе практических и лабораторных занятий<br>1. Настройка безопасного хранилища<br>2. Проверка на утечки с помощью MobSF<br>3. Защита от подмены интентов<br>4. Эмуляция MITM и его предотвращение<br>5. Работа с разрешениями на уровне кода<br>6. Защита файлов и кеша (internal/external storage) | 10 | 14 | - | ОК.01 – ОК.09, ПК 3.1 – ПК 3.7 | Т, ПЗ, О |
| 2 | Тема 1.2. Аутентификация и безопасный обмен | **Содержание учебного Материала** Авторизация: OAuth2, OpenID, токены<br>Хранение и валидация токенов<br>Работа с биометрией: Fingerprint API, Face ID | 10 | 14 | - | ОК.01 – ОК.09, ПК 3.1 – ПК 3.7 | Т, ПЗ, О |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Безопасная передача данных (HTTPS, SSL Pinning)<br>В том числе практических и лабораторных занятий<br>1. Интеграция входа по биометрии<br>2. Работа с JWT и обновление access токенов<br>3. Настройка SSL Pinning в приложении<br>4. Интеграция аутентификации через внешние API<br>5. Обработка 401/403 ответов и авто-логаут<br>6. Проверка безопасности данных при межприложенном взаимодействии | | | | | |
| 3 | Тема 1.3. Аудит и hardening | **Содержание учебного материала**<br>Инструменты анализа безопасности: MobSF, OWASP<br>Проверка на рут/джейлбрейк<br>Обфускация кода: ProGuard, R8<br>Хардкорный hardening: SELinux, AppArmor, Seccomp<br>Политики безопасности в Aurora и РЕД ОС<br>Безопасность CI/CD пайплайна<br>В том числе практических и лабораторных занятий<br>1. Анализ apk через MobSF<br>2. Внедрение ProGuard<br>3. Проверка root-статуса устройства<br>4. Интеграция обфускации в CI<br>5. Проверка соответствия требованиям безопасной разработки<br>6. Реализация политики безопасности под РЕД ОС | 12 | 12 | | ОК.01 – ОК.09, ПК 3.1 – ПК 3.7 | Т, ПЗ, О |
| | | Итого часов: | 22 | 34 | - | | |

### 2.3. Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в Таблице 2.3.

Таблица 2.3. — Распределение видов учебной работы и текущей аттестации

| **Вид учебной работы** | **Формат проведения** |
|---|---|
| Лекционные занятия | Частично с применением ДОТ |
| Практические занятия | Частично с применением ДОТ |
| Текущий контроль | Частично с применением ДОТ |

| | |
|---|---|
| Промежуточная аттестация | Контактная аудиторная работа |
| **Формы текущего контроля** | **Формат проведения** |
| Тестирование | Частично с применением ДОТ |
| Опрос | Контактная аудиторная работа |
| Практические задания | Частично с применением ДОТ |

Доступ к системе дистанционных образовательных программ осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://sziu-de.ranepa.ru, в соответствии с их индивидуальным паролем и логином к личному кабинету/ профилю.

Текущий контроль, проводимый в системе дистанционного обучения, оцениваются как в системе дистанционного обучения, так и преподавателем вне системы.

Доступ к материалам лекций предоставляется в течение всего семестра по мере прохождения освоения программы. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется ограниченное время согласно регламенту дисциплины, опубликованному в системе дистанционного обучения. Преподаватель оценивает выполненные обучающимися работы не позднее 14 рабочих дней после окончания срока выполнения.

## 3 Материалы текущего контроля успеваемости и промежуточной аттестации обучающихся

### 3.1 Формы и методы текущего контроля успеваемости и промежуточной аттестации обучающихся

Формы текущего контроля успеваемости:

**Опрос (О**) позволяет выявить правильность ответа по содержанию, его последовательность, самостоятельность суждений и выводов, степень развития логического мышления.

**Тестирование (Т)** – задания, с вариантами ответов.

**Практическое задание (ПЗ)** используется для закрепления теоретических знаний и отработки навыков и умений, способности применять знания при решении конкретных задач.

**Критерии оценивания форм текущей и промежуточной аттестаций:**

Оценки «отлично» заслуживает студент, обнаруживший глубокое знание материала, умение свободно выполнять задания, понимающий взаимосвязь основных понятий темы; в тесте студент ответил правильно на 90-100% вопросов теста;

Оценки «хорошо» заслуживает студент, обнаруживший полное знание материала; успешно выполняющий предусмотренные задания; и допустивший незначительные ошибки: неточность фактов, стилистические ошибки; в тесте студент ответил правильно на 89-75% вопросов теста;

Оценки «удовлетворительно» заслуживает студент, обнаруживший знания основного материала в объеме, необходимом для дальнейшего изучения дисциплины. Справляющийся с выполнением заданий; допустивший погрешности в ответе, но обладающий необходимыми знаниями для их устранения под руководством преподавателя; в тесте студент ответил правильно на 74-50% вопросов теста;

Оценки «неудовлетворительно» заслуживает студент, обнаруживший существенные пробелы в знании основного материала; не справляющийся с выполнением заданий, допустивший серьезные погрешности в ответах, нуждающийся в повторении основных разделов курса под руководством преподавателя. в тесте студент ответил правильно менее чем 49% вопросов теста;

**Формы текущего контроля**

| № п/п | Название темы | Формы текущего контроля успеваемости |
|---|---|---|
| 1 | Тема 1.1. Угрозы и модели безопасности | Т, ПЗ, О |
| 2 | Тема 1.2. Аутентификация и безопасный обмен | Т, ПЗ, О |
| 3 | Тема 1.3. Аудит и hardening | Т, ПЗ, О |

Примечание. В столбце «Форма текущего контроля успеваемости, промежуточной аттестации» перечисляются все используемые в учебном процессе по данной дисциплине формы контроля освоения материала. (Т – тестирование; ПЗ – практическое задание, О - опрос).

## 3.2 Оценочные средства текущего контроля успеваемости обучающихся

### Примеры типовых заданий для практических работ
### Тема 1.1. Угрозы и модели безопасности

1. **Настройка безопасного хранилища**. Задание: реализуйте хранение чувствительных данных (токен доступа, PIN-код) в приложении:

- используйте `EncryptedSharedPreferences` для простых значений;
- для более критичных данных примените Android Keystore для генерации и хранения криптографического ключа;

- напишите код для шифрования/дешифрования данных с этим ключом.

Приложите фрагменты кода (инициализация хранилища, операции записи/чтения, работа с Keystore), скриншоты или логи, подтверждающие, что данные не читаются в файловой системе (например, через adb). Кратко (3–4 предложения) объясните, в чём разница между обычным SharedPreferences и EncryptedSharedPreferences, и когда оправдано использование Keystore.

2. **Проверка на утечки с помощью MobSF**. Задание: подготовьте APK-файл учебного приложения и просканируйте его в MobSF:

- соберите отчёт по уязвимостям (Hardcoded secrets, Weak crypto, Permissions issues и т. п.);
- выделите 3–5 критичных проблем и исправьте их в коде;
- повторно просканируйте и покажите улучшение.

Приложите скриншоты отчётов «до» и «после», список исправленных уязвимостей и краткое описание внесённых изменений. Кратко (2–3 предложения) сформулируйте, как регулярное использование MobSF помогает соблюдать принципы безопасной разработки.

3. **Защита от подмены интентов**. Задание: смоделируйте и предотвратите атаку на подмену Activity:

- создайте два приложения: «отправитель» (запускает интент) и «получатель» (обрабатывает интент);
- продемонстрируйте сценарий, когда злоумышленное приложение перехватывает интент;
- реализуйте защиту: явные интенты, проверка подписи пакета, ограничение экспортируемости компонента.

Приведите код манифеста, отправки/приёма интента и описание тестов. Кратко (3–4 предложения) объясните, какие механизмы Android защищают от подмены компонентов и в каких случаях их недостаточно.

4. **Эмуляция MITM и его предотвращение**. Задание: проведите контролируемую проверку защиты сетевого трафика:

- в тестовой среде установите пользовательский сертификат и перехватите HTTPS-трафик (например, с помощью mitmproxy);
- зафиксируйте, что приложение принимает поддельный сертификат;
- внедрите SSL Pinning (закрепление сертификата) и повторно протестируйте перехват;

- покажите, что трафик больше не расшифровывается.

Приложите команды установки сертификата, конфиг для pinning, скриншоты перехвата «до» и «после». Кратко (3–4 предложения) опишите ограничения и риски использования SSL Pinning в продакшене.

5. **Работа с разрешениями на уровне кода**. Задание: реализуйте корректную обработку runtime-разрешений:

- запросите доступ к камере и хранилищу, обработайте сценарии «разрешено», «отклонено», «всегда отклонено»;
- при «всегда отклонено» покажите понятное объяснение пользователю и перенаправление в настройки;
- добавьте логирование всех состояний и обработку edge-case (например, отзыв разрешения в настройках).

Приложите код запроса, обработки результата и примеры логов. Кратко (2–3 предложения) поясните, как правильная работа с пермишенами снижает риски утечки данных и улучшает UX.

6. **Защита файлов и кеша (internal/external storage)**. Задание: сравните хранение данных во внутреннем и внешнем хранилище:

- сохраните тестовый файл в internal storage и external storage;
- проверьте доступность файлов из других приложений и через adb;
- реализуйте шифрование файла и хранение метаданных в защищённом хранилище.

Приложите код, команды проверки доступа, результаты тестов. Кратко (3–4 предложения) сформулируйте рекомендации по выбору места хранения для разных типов данных (кеш, медиа, секреты).

## Примеры тестовых заданий

### Часть 1. Задания с выбором одного правильного ответа

1. Что обеспечивает SSL Pinning?

а) Автоматическое обновление сертификатов сервера

б) Принудительную проверку конкретного сертификата (или его хэша) при установке соединения

в) Шифрование данных на устройстве

г) Защиту от утечки токенов через Intent

2. Какой механизм Android позволяет хранить криптографические ключи, недоступные другим приложениям и даже ОС (в аппаратном анклаве)?

а) SharedPreferences

б) Internal Storage

в) Android Keystore

г) EncryptedSharedPreferences

3. Что означает код ответа HTTP 401 в контексте аутентификации?

а) Сервер не нашёл запрашиваемый ресурс

б) У пользователя нет прав на доступ к ресурсу

в) Требуется аутентификация, токен отсутствует или истёк

г) Сервер временно недоступен

**Часть 2. Задания на установление соответствия**

Установите соответствие между угрозой и способом защиты:

| Угроза | Способ защиты |
|---|---|
| 1. MITM-атака | А. SSL Pinning, HTTPS с валидными сертификатами |
| 2. Утечка токенов через логи | Б. Исключение чувствительных данных из логов, использование безопасных уровней логирования |
| 3. Подмена Activity | В. Явные интенты, ограничение экспортируемости, проверка подписи вызывающего приложения |
| 4. Реверс-инжиниринг кода | Г. Обфускация (ProGuard/R8), минимизация отладочной информации |

**Часть 3. Задания на последовательность действий**

Установите правильную последовательность шагов при безопасной обработке истечения токена (401):

а) Получить новый access-токен по refresh-токену

б) Повторно выполнить исходный запрос с новым access-токеном

в) Обнаружить ответ 401 от сервера

г) Если обновление не удалось — очистить сессию и перенаправить на экран входа

д) Сохранить новый access-токен в защищённом хранилище

**Часть 4. Ситуационные задачи**

В приложении обнаружены жёстко прописанные ключи API и пароли в коде. Какие шаги вы предпримете для устранения уязвимости? Опишите план из 5–7 пунктов, включая инструменты и изменения в архитектуре.

Приложение должно работать в защищённой среде РЕД ОС и не должно допускать запуск на рутованных устройствах. Предложите архитектуру решения: какие проверки и ограничения нужны, как обрабатывать обнаружение рута, как согласовать это с требованиями к UX. Приведите краткий план реализации (6–8 пунктов).

Вы готовите релизную сборку приложения для публикации. Перечислите 5–6 обязательных шагов по hardening, которые нужно выполнить перед релизом, и укажите, какие инструменты или настройки для этого использовать (MobSF, ProGuard, SSL Pinning и т. д.).

**Примеры типовых вопросов для устного опроса**

1. Расскажите, какие угрозы покрывает модель угроз Android и как они отличаются от угроз в Aurora/РЕД ОС.
2. Объясните разницу между хранением секретов в SharedPreferences, EncryptedSharedPreferences и Android Keystore, и приведите пример, когда нужно использовать каждый вариант.
3. Как работает SSL Pinning и какие риски он несёт при неправильной реализации?
4. Опишите типичный поток OAuth2 с PKCE и объясните, зачем нужен PKCE.
5. Какие механизмы Android помогают защититься от подмены компонентов (Activity, Service) и в каких сценариях их недостаточно?
6. Что такое OWASP Mobile Top 10 и как эти риски проявляются в мобильных приложениях?
7. Как обфускация кода (ProGuard/R8) усложняет анализ приложения и какие проблемы она может вызвать?
8. Как проверить, что приложение не имеет уязвимостей, связанных с межприложенным взаимодействием? Приведите 3–4 конкретных проверки.
9. Какие политики безопасности в РЕД ОС отличают её от стандартного Android, и как адаптировать приложение под эти требования?
10. Как интегрировать проверки безопасности в CI/CD пайплайн и какие этапы обязательно нужно автоматизировать?

### 3.3 Оценочные средства по дисциплине для промежуточной аттестации

Зачет с оценкой проводится в устной форме по вопросам из перечня.

**Вопросы для подготовки к зачету с оценкой**

1. Что такое модель угроз Android и как она отличается от модели угроз Aurora?

2. Какие основные принципы защищённой архитектуры мобильного приложения?
3. Как работает EncryptedSharedPreferences и где его применять?
4. В чём особенности Android Keystore и как его настроить?
5. Какие существуют уровни разрешений (пермишенов) в Android?
6. Как предотвратить MITM-атаки в мобильном приложении?
7. Какие методы защиты от инжекции кода существуют?
8. Как защититься от подмены Activity?
9. Какие особенности защиты реализованы в РЕД ОС М?
10. Как использовать MobSF для проверки безопасности приложения?
11. Что такое OAuth2 и как он работает?
12. В чём суть протокола OpenID?
13. Как правильно хранить JWT-токены?
14. Как реализовать валидацию токенов в приложении?
15. Какие API используются для работы с биометрией?
16. Как настроить Fingerprint API?
17. Что такое SSL Pinning и зачем он нужен?
18. Как реализовать безопасную передачу данных через HTTPS?
19. Как обрабатывать 401/403 ответы?
20. Что такое авто-логаут и как его реализовать?
21. Какие инструменты анализа безопасности существуют?
22. Как проверить устройство на рут-доступ?
23. Что такое джейлбрейк и как его обнаружить?
24. Как работает ProGuard?
25. В чём отличие ProGuard от R8?
26. Что такое SELinux и как его настроить?
27. Как работает AppArmor?
28. Для чего нужен Seccomp?
29. Какие политики безопасности существуют в Aurora?
30. Как обеспечить безопасность CI/CD пайплайна?
31. Как защитить файлы во внутреннем хранилище?
32. Какие методы защиты внешнего хранилища существуют?
33. Как проверить приложение на утечки данных?
34. Что такое обфускация кода и зачем она нужна?

35. Как внедрить политику безопасности в РЕД ОС?
36. Какие методы защиты от декомпиляции существуют?
37. Как реализовать защиту от отладки?
38. Что такое root-проверка и как её реализовать?
39. Как защитить приложение от анализа дизассемблером?
40. Какие существуют методы защиты от реверсинжиниринга?
41. Как реализовать безопасное хранение паролей?
42. Что такое токен-based аутентификация?
43. Как реализовать двухфакторную аутентификацию?
44. Какие методы защиты от брутфорс-атак существуют?
45. Как обеспечить безопасность при межприложенном взаимодействии?
46. Что такое безопасное хранилище и как его настроить?
47. Как реализовать защиту от SQL-инъекций?
48. Какие методы защиты от XSS-атак существуют?
49. Как обеспечить безопасность при работе с API?
50. Какие требования к безопасности CI/CD процессов существуют?

## 4. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению дисциплины «Технология безопасности мобильных платформ», студент должен ознакомиться с содержанием данной «Рабочей учебной программы дисциплины» с тем, чтобы иметь четкое представление о своей работе.

В первую очередь необходимо уяснить цель и задачи изучаемой дисциплины, оценить объем материала, познакомиться с предложенной и подобрать основную и дополнительную литературу, выявить наиболее важные проблемы, стоящие по вопросам изучаемой дисциплины.

Выполнение заданий осуществляется в соответствии с учебным планом и программой. Они должны выполняться в соответствии с методическими рекомендациями, выданными преподавателем, и представлены в установленные преподавателем сроки.

Работая с учебниками и учебными пособиями, целесообразно законспектировать тот материал, который не сообщался студентам на лекциях.

На занятиях лекционного и практического характера студентам для работы требуется: тетрадь для записи лекций и заданий.

Для успешного овладения программой дисциплины необходимо выполнять следующие требования:

- посещать все лекционные и практические занятия;
- все рассматриваемые на лекциях и практических занятиях темы и вопросы обязательно фиксировать в тетради;
- в случае пропуска занятий по каким-либо причинам необходимо обязательно самостоятельно изучать соответствующий материал в Moodle, фиксируя записи в тетради, а также выполнять практические задания.

Подготовка к зачету с оценкой осуществляется по представленным в списке основной и дополнительной литературе. Рекомендуемые литература и интернет-ресурсы будут полезны при выполнении практических заданий и для подготовки к тестированиям.

Методические рекомендации по составлению конспекта

Конспект — сложный способ изложения содержания книги или статьи в логической последовательности. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта. Выделите главное, составьте план, представляющий собой перечень заголовков, подзаголовков, вопросов, последовательно раскрываемых затем в конспекте.

Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

При оформлении конспекта необходимо стремиться к емкости каждого предложения.

Методические рекомендации по составлению опорного конспекта

Опорный конспект — вид внеаудиторной самостоятельной работы студента по созданию краткой информационной структуры, обобщающей и отражающей суть материала лекции, темы учебника.

Опорный конспект — это наилучшая форма подготовки к ответу на вопросы.

Основная цель опорного конспекта — облегчить запоминание. Этапы составления опорного конспекта:

1. Изучить материалы темы, выбрать главное и второстепенное;
2. Установить логическую связь между элементами темы;
3. Представить характеристику элементов в краткой форме;
4. Выбрать опорные сигналы для акцентирования главной информации и отобразить в структуре работы.

Методические рекомендации по прохождению тестирования

Тестирование — это исследовательский метод, который позволяет выявить уровень знаний, умений и навыков, способностей, а также их соответствие определенным нормам усвоения, путем выполнения испытуемым ряда специальных заданий.

Следует понимать, что тестовые задания могут быть представлены в различных формах:

− задания закрытой формы, в которых обучающийся выбирает один или несколько правильных ответов из заданного набора:

− задания на дополнение (открытые задания), требующие самостоятельного получения ответов:

− задания на установления соответствия (с множественным выбором), выполнение которых связано с выявлением соответствия между элементами нескольких множеств:

− задания на установление правильной последовательности, в которых от учащегося требует указать порядок действий или процессов и другие. Этапы подготовки к тестированию:

1. Внимательно прочитайте материал по конспекту, составленному на учебном занятии. Прочитайте тот же материал по учебнику, учебному пособию.

2. Постарайтесь разобраться с непонятным, в частности новыми терминами и конструкциями.

3. Ответьте на контрольные вопросы для самопроверки, имеющиеся в учебнике, конспекте и т. д.

4. Кратко перескажите содержание изученного материала «своими словами».

5. Выучите определения основных понятий, условные обозначения, формулы и конструкции.

Подготовка к практическим занятиям

В ходе подготовки к практическим занятиям необходимо изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях, ознакомиться с программным обеспечением. Следует дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Заканчивать подготовку следует закреплением материала с использованием соответствующих программных продуктов.

Все практические задания, предусмотренные рабочей программой, представлены в фонде оценочных средств по дисциплине.

Критерии оценивания выполненных практических работ:

− правильность выполнения работы (отсутствие фактических, логических и других ошибок);

- полнота выполнения работы;
- своевременность выполнения;
- правильность оформления отчета.

За задания, выполненные позже установленного срока или с нарушениями требований к оформлению, оценка на балл снижается.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Целью самостоятельной работы студентов является: овладение практическими знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой, исследовательской деятельности.

Самостоятельная работа студентов предполагает:

- самостоятельный поиск ответов и необходимой информации в рамках изучаемых тем;
- выполнение заданий для самостоятельной работы, в том числе тестов;
- изучение теоретического и лекционного материала, а также основной и дополнительной литературы при подготовке к практическим занятиям.

## 5 Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

**Основная литература**

1. Введение в разработку приложений для ОС Android : учебное пособие для СПО / Ю. В. Березовская, О. А. Юфрякова, В. Г. Вологдина [и др.]. — 2-е изд. — Саратов : Профобразование, 2024. — 427 с. — ISBN 978-5-4488-0993-4. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/139746

2. Семакова, А. Введение в разработку приложений для смартфонов на ОС Android : учебное пособие для СПО / А. Семакова. — 2-е изд. — Саратов : Профобразование, 2024. — 102 с. — ISBN 978-5-4488-0994-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/139747

3. 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 // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/121301

## 6 Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

***Для реализации дисциплины необходимы:***

− рабочие станции (персональные компьютеры) с характеристиками не ниже: процессор — Intel Core i5 (или аналогичный AMD), ОЗУ — 16 ГБ, SSD — не менее 256 ГБ;

− проекционное оборудование (проектор/интерактивная доска) для демонстрации материалов;

− сетевое подключение со скоростью не менее 100 Мбит/с.

***Программное обеспечение***

Операционные системы: Windows 10/11, Linux (Ubuntu, CentOS, Astra, Alt)

Офисные пакеты: Microsoft Office 365, LibreOffice

***Электронно-библиотечные системы (ЭБС)***

1. ЭБС «BOOK.RU». — URL: https://book.ru/
2. ЭБС «Znanium». — URL: https://znanium.ru/
3. ЭБС «Айбукс». — URL: https://ibooks.ru/
4. ЭБС «Лань». — URL: https://e.lanbook.com/
5. ЭБС «Юрайт». — URL: https://urait.ru/
6. Электронные каталоги библиотеки СЗИУ РАНХиГС. — URL: https://sziu-lib.ranepa.ru/