МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность мобильных устройств

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

ДУШАНБЕ - 2026

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Безопасность мобильных устройств для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Кафедра информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Актуальность изучения дисциплины «Безопасность мобильных устройств»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Безопасность мобильных устройств" является формирование у студентов теоретических знаний и практических навыков в области защиты мобильных устройств от различных угроз, обеспечение конфиденциальности данных и поддержание безопасности информационных систем. Дисциплина направлена на подготовку специалистов, способных оценивать риски безопасности, разрабатывать и применять меры защиты, а также реагировать на инциденты, связанные с безопасностью мобильных устройств. В результате изучения дисциплины студенты должны овладеть современными методами и технологиями обеспечения безопасности мобильных платформ.

1.2 Задачи изучения дисциплины Изучение основных угроз безопасности мобильных устройств. Ознакомление с архитектурой и особенностями операционных систем мобильных устройств. Формирование навыков анализа уязвимостей и разработки мер защиты. Изучение методов защиты данных, хранящихся на мобильных устройствах. Освоение инструментов и технологий для обеспечения безопасности мобильных приложений.

1.3 В результате изучения дисциплины «Безопасность мобильных устройств» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
ПК-2	Способен разрабатывать и адаптировать прикладное программное обеспечение	ИПК-2.1 Применяет современные технологии разработки и адаптации прикладного ПО.ИПК-2.2 Разрабатывает и адаптирует ПО на современных языках программирования.ИПК-2.3 Применяет современные технологии для разработки веб-приложений.	

ПК-3	Способен проектировать информационные системы по видам обеспечения	ИПК-3.1 Обосновывает выбор проектных решений по видам обеспечения ИС.ИПК-3.2 Участвует в проектировании экономических ИС и их модулей.	
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.1 Формулирует совокупность взаимосвязанных задач. ИУК-2.2 Определяет ресурсное обеспечение. ИУК-2.3 Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач. ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Безопасность мобильных устройств»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.03).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

2.2 Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

№ п/п	**Название дисциплины**	**Семестр**	**Место дисциплины в структуре ОПОП**
-	—	—	Предшествующая дисциплина
-	—	—	Последующая дисциплина

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2.

Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Безопасность мобильных устройств» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 72 часа, из которых: лекции – 14 часов, практические занятия – 14 часов, лабораторные работы 8 часов, иная контактная работа – 32 часа, самостоятельная работа – 44. Всего часов аудиторной нагрузки – 28 часа.

По итогам 4 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в безопасность мобильных устройств. Обзор угроз и уязвимостей.

Основные понятия и определения. Классификация угроз. Статистика угроз безопасности мобильных устройств. Обзор уязвимостей.

Лекция 2 Архитектура мобильных операционных систем (Android, iOS).

Обзор архитектуры Android и iOS. Сравнение подходов к безопасности в Android и iOS.

Лекция 3 Атаки на мобильные устройства: вредоносное ПО, фишинг, социальная инженерия.

Виды вредоносного ПО. Методы фишинга. Приемы социальной инженерии. Примеры атак.

Лекция 4 Безопасность приложений. Жизненный цикл мобильного приложения.

Обзор проблем безопасности мобильных приложений. Жизненный цикл мобильного приложения с точки зрения безопасности.

Лекция 5 Методы защиты данных на мобильных устройствах. Шифрование.

Защита данных при хранении и передаче. Шифрование данных. Практические примеры.

Лекция 6 Аутентификация и авторизация в мобильных приложениях.

Методы аутентификации. Различные типы авторизации. Безопасные методы хранения учетных данных.

Лекция 7 Безопасность беспроводных сетей (Wi-Fi, Bluetooth).

Угрозы безопасности в беспроводных сетях. Методы защиты.

Структура и содержание практической части курса

Структура и содержание лабораторной части курса

Лабораторная работа 1 Сканирование уязвимостей мобильного приложения с использованием инструментов.

Практическое занятие по использованию инструментов для сканирования уязвимостей в мобильных приложениях.

Лабораторная работа 2 Перехват и анализ сетевого трафика мобильного приложения.

Практическое занятие по перехвату и анализу сетевого трафика мобильных приложений.

Лабораторная работа 3 Реверс-инжиниринг мобильного приложения.

Практическое занятие по реверс-инжинирингу мобильных приложений для выявления уязвимостей.

Лабораторная работа 4 Разработка безопасного мобильного приложения.

Практическое занятие по разработке безопасного мобильного приложения (простейший пример).

Структура и содержание КСР

КСР 1 Анализ безопасности мобильного приложения.

Анализ конкретного мобильного приложения с точки зрения безопасности, выявление уязвимостей и разработка рекомендаций по их устранению.

КСР 2 Разработка политики безопасности для мобильного устройства.

Разработка политики безопасности для мобильного устройства в организации.

КСР 3 Сравнение инструментов для тестирования безопасности мобильных приложений.

Сравнение различных инструментов тестирования безопасности мобильных приложений, оценка их возможностей и областей применения.

Структура и содержание СРС

СРС 1 Изучение современных угроз безопасности мобильных устройств.

Самостоятельное изучение актуальных угроз и способов защиты от них.

СРС 2 Изучение методов защиты информации на мобильных устройствах.

Самостоятельное изучение методов шифрования, аутентификации и авторизации.

СРС 3 Анализ уязвимостей мобильных приложений.

Изучение уязвимостей мобильных приложений и способов их эксплуатации.

СРС 4 Работа с инструментами для анализа безопасности мобильных приложений.

Самостоятельное изучение и освоение инструментов для тестирования безопасности мобильных приложений.

СРС 5 Подготовка презентации по теме "Безопасность мобильных платежей".

Подготовка презентации, включающей обзор технологий, угроз и методов защиты мобильных платежей.

СРС 6 Написание реферата по теме "Защита мобильных устройств от вредоносного ПО".

Подготовка реферата, посвященного вредоносному ПО для мобильных устройств, способам его распространения и методам защиты.

СРС 7 Изучение и сравнение различных мобильных операционных систем с точки зрения безопасности.

Самостоятельное изучение подходов к безопасности в различных мобильных операционных системах.

СРС 8 Разработка плана мероприятий по обеспечению безопасности мобильных устройств в организации.

Разработка плана мероприятий, направленного на обеспечение безопасности мобильных устройств в организации.

СРС 9 Подготовка обзора современных инструментов аудита безопасности мобильных приложений.

Подготовка обзора современных инструментов аудита безопасности мобильных приложений, оценка их функциональности и применимости.

СРС 10 Изучение различных стандартов и рекомендаций по безопасности мобильных устройств (OWASP, NIST).

Изучение стандартов и рекомендаций, применяемых для обеспечения безопасности мобильных устройств, анализ их практического применения.

СРС 11 Анализ существующих угроз безопасности и разработка мер противодействия.

Самостоятельный анализ существующих угроз безопасности мобильных устройств и разработка эффективных мер противодействия.

СРС 12 Изучение методов защиты данных при передаче по сети на мобильных устройствах.

Самостоятельное изучение протоколов и методов обеспечения безопасности при передаче данных по сети на мобильных устройствах.

СРС 13 Разработка безопасного мобильного приложения с использованием современных фреймворков и библиотек.

Практическая работа по разработке безопасного мобильного приложения с учетом требований к безопасности.

СРС 14 Исследование уязвимостей в конкретном мобильном приложении и разработка способов их устранения.

Практическое исследование уязвимостей в существующем мобильном приложении и разработка конкретных мер по их устранению.

СРС 15 Подготовка отчета об аудите безопасности мобильного приложения.

Подготовка подробного отчета об аудите безопасности мобильного приложения, включая описание обнаруженных уязвимостей и рекомендации по их устранению.

СРС 16 Самостоятельное изучение передовых технологий защиты мобильных устройств.

Самостоятельное изучение передовых технологий, таких как биометрическая аутентификация, шифрование на уровне устройства и т.д.

СРС 17 Подготовка обзора современных решений для управления мобильными устройствами (MDM).

Изучение функциональности, преимуществ и недостатков различных MDM-решений, анализ их применимости в различных сценариях.

СРС 18 Разработка сценария тестирования безопасности мобильного приложения.

Разработка подробного сценария тестирования безопасности мобильного приложения, включающего различные виды проверок и тестов.

СРС 19 Анализ и оценка эффективности различных методов защиты от фишинга на мобильных устройствах.

Исследование методов борьбы с фишингом на мобильных устройствах, оценка их эффективности и разработка рекомендаций по их применению.

СРС 20 Подготовка презентации о лучших практиках разработки безопасных мобильных приложений.

Разработка презентации о лучших практиках разработки безопасных мобильных приложений, с акцентом на применение актуальных инструментов и технологий.

СРС 21 Исследование и анализ способов обхода защиты на мобильных устройствах.

Анализ современных способов обхода защиты, применяемых злоумышленниками для получения несанкционированного доступа к данным.

СРС 22 Практическое применение инструментов для анализа безопасности мобильного приложения.

Практическое освоение и применение инструментов для анализа безопасности мобильных приложений, включая статический и динамический анализ.

Структура и содержание теоретической, лабораторной части курса, КСР и СРС

Таблица 3.

№ п/п	Наименование темы	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Литра	Количество баллов
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в безопасность мобильных устройств. Обзор угроз и уязвимостей.	2				4		1,5,6	12,5
2	Сканирование уязвимостей мобильного приложения с использованием инструментов.				2	4		1,2	12,5
3	Архитектура мобильных операционных систем (Android, iOS).	2				4		2,3	12,5
4	Анализ безопасности мобильного приложения.		2			4		5,7	12,5
5	Атаки на мобильные устройства: вредоносное ПО, фишинг, социальная инженерия.	2				4		7,5,6	12,5
6	Перехват и анализ сетевого трафика мобильного приложения.				2			1,3,5	12,5
7	Безопасность приложений. Жизненный цикл мобильного приложения.	2				4		4,7,5	12,5
8	Разработка политики безопасности для мобильного устройства.		2			4		5,2,3	12,5
9	Методы защиты данных на мобильных устройствах. Шифрование.	2				4		3,2	12,5
10	Реверс-инжиниринг мобильного приложения.				2			2,4	12,5

11	Аутентификация и авторизация в мобильных приложениях.	2				4		7,5	12,5
12	Сравнение инструментов для тестирования безопасности мобильных приложений.		2			4		6,2	12,5
13	Безопасность беспроводных сетей (Wi-Fi, Bluetooth).	2				4		4,5	12,5
14	Разработка безопасного мобильного приложения.				2			1,7	12,5
Итого:		**14**	**6**	**0**	**8**	**44**			**175**

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **2 -го курса**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, экзамен) проводится как в

форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

Таблица 4.

Неделя	Активное участие на лекционных занятиях, написание конспекта и выполнение других видов работ*	Активное участие на практических (семинарских) занятиях, КСР	СРС Написание реферата, доклада, эссе Выполнение других видов работ	Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы)	РК №1	Всего
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Первый рейтинг	21	31,5	17,5	17,5	12,5	100
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Второй рейтинг	21	31,5	17,5	17,5	12,5	100
Итог						200

Формула вычисления результатов дистанционного контроля и итоговой формы контроля по дисциплине за семестр для студентов 2 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

где ИБ –итоговый балл, P_1- итоги первого рейтинга, P_2- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

3. требования к представлению и оформлению результатов самостоятельной работы;

4. критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

4.1. План-график выполнения самостоятельной работы по дисциплине

№	Объем СРС, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Понятие и особенности безопасности мобильных устройств	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Архитектура мобильных операционных систем	Вопросы 5–8. Презентация методов	Выступление
3	6	Модель угроз для мобильных устройств	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Уязвимости мобильных операционных систем	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Политики безопасности мобильных устройств	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Средства аутентификации и контроля доступа	Выполнение задания 2	Защита работы

7	6	Защита мобильных приложений	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Защита данных на мобильных устройствах	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Антивирусные и антишпионские средства	Выполнение задания 5	Защита работы
10	4	Безопасность беспроводных соединений	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Управление мобильными устройствами (MDM)	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Реагирование на инциденты безопасности	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Правовые аспекты безопасности мобильных устройств	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Тестирование безопасности мобильных приложений	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Безопасность BYOD-среды	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексная система защиты мобильных устройств	Вопросы 45–46. Выполнение задания 8 (4–10)	Защита работы

4.2 Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в лекционной (практической) тетради в произвольной форме.

4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература:

1. 1. Власов С.В. Безопасность мобильных устройств: учебное пособие. М.: Юрайт, 2020. 200 стр.
2. Комаров В.И., Кузнецов А.А. Защита информации в мобильных системах. СПб.: Питер, 2019. 256 стр.
3. Райхман Д.А. Основы кибербезопасности мобильных приложений. М.: ДМК Пресс, 2019. 300 стр.
4. Курбанов Р.А., Скворцов А.В. Безопасность операционных систем мобильных устройств. М.: Флинта, 2020. 224 стр.
5. Самсонов А.В., Иванов М.А. Анализ уязвимостей мобильных приложений. СПб.: БХВ-Петербург, 2019. 180 стр.
6. Бобров А.А. Практикум по безопасности мобильных устройств. М.: Солон-Пресс, 2018. 160 стр.
7. Липкин М.Ю. Аудит безопасности мобильных платформ. М.: Курс, 2018. 288 стр.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Кроль Ю.А. Безопасность мобильных сетей. М.: Горячая линия - Телеком, 2017.
2. Романец Ю.В., Тимофеева Л.П., Петров А.М. Защита информации в компьютерных системах и сетях. М.: Горячая линия - Телеком, 2019.

3. Щербаков А.Ю. Информационная безопасность: учебное пособие. М.: КноРус, 2018.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2016.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2017.
6. Корольков А.В. Основы защиты информации: учебное пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2016.
7. Ситников А.Е. Методы и средства защиты информации. М.: Академия, 2015.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. OWASP Mobile Security Project: https://owasp.org/www-project-mobile-top-10/
2. Android Developers: https://developer.android.com/
3. Apple Developer: https://developer.apple.com/
4. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
5. SANS Institute: https://www.sans.org/

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Безопасность мобильных устройств» и успешного прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные

формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Безопасность мобильных устройств» строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине «Безопасность мобильных устройств» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы,

контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ

ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	Диапазон соответствующих наборных баллов	Численное выражение оценочного балла	Оценка по традиционной системе
A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	Неудовлетворительно
F	0	0-44	

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.