БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям

_____ О.Г. Прохоренко

30 июня 2023 г.

Регистрационный № УД -12486/уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Учебная программа учреждения высшего образования по учебной дисциплине для специальностей:

1-31 03 07 Прикладная информатика (по направлениям)
Направление специальности:
1-31 03 07 - 01 Прикладная информатика (программное обеспечение компьютерных систем)

2023 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-31 03 07-2021, типового учебного плана G 31-1-030/пр-тип от 01.07.2021., учебного плана БГУ G 31-1-034/уч. от 23.07.2021, учебного плана БГУ G 31-1-023/уч. ин. от 09.08.2021

СОСТАВИТЕЛЬ:

А.В.Федчук, старший преподаватель кафедры технологий программирования факультета прикладной математики и информатики белорусского государственного университета

РЕЦЕНЗЕНТ:

А.В.Решетняк, заместитель технического директора Государственного предприятия «Центр Систем Идентификации»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования факультета прикладной математики и информатики
(протокол № 16 от 18 мая 2023 г.)

Научно-методическим советом БГУ
(протокол № 9 от 29.06.2023)

Заведующий кафедрой _____ А.Н.Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель преподавания дисциплины «Информационная безопасность мобильных приложений» является грамотный анализ уязвимостей системы таким образом, чтобы эффективно выявлять слабые места и предотвращать утечку информации.

Задачи учебной дисциплины:

- проводить аудит безопасности мобильных устройств;
- изучить принципы устройства операционных систем iOS и Android;
- получить навыки основ разработки и функционирования мобильного ПО;
- уметь выполнять статический и динамический анализ кода;
- работать с самыми распространенными уязвимостями мобильных приложений по классификации OWASP Mobile Top 10;
- получить навыки контроля межпроцессного и сетевого взаимодействия мобильных приложений.

Место учебной дисциплины

Дисциплина «Информационная безопасность мобильных приложений» относится к циклу дисциплин специализации и разработана в соответствии с учебным планом и образовательным стандартом первой ступени высшего образования по специальности 1-31 03 07 Прикладная информатика.

Дисциплины, являющиеся основой для курса: алгоритмизация и основы программирования, информатика, программирование на языке ассемблера, программирование на языке С/С++, технологии программирования, инструментальные средства разработки программ, архитектура компьютерных систем, сетевое программирование.

Требования к компетенциям

Освоение учебной дисциплины Информационная безопасность мобильных приложений» должно обеспечить формирование следующих компетенций:

Универсальные компетенции

УК-1 Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации;

УК-2 Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий;

УК-4 Работать в команде, толерантно воспринимать социальные, этнические, конфессиональные, культурные и иные различия;

УК-6 Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности.

Базовые профессиональные компетенции

БПК-2. Строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования.

Специализированные компетенции

СК-5 Использовать программные средства и технологии для создания прикладного программного обеспечения;

СК-13 Разрабатывать программное обеспечение в интегрированных средах разработки.

В результате изучения дисциплины студент должен:

знать:

- основные подходы к защите данных;
- архитектуру мобильных приложений;
- внутреннюю структуру мобильной ОС;

уметь:

- оценивать эффективность защиты данных;
- искать причины ослабления средств защиты.

владеть:

- навыками оценки надежности алгоритмов и протоколов;
- методами и практическим применением защиты ядра ОС;

Структура учебной дисциплины.

Дисциплина изучается в шестом семестре. Всего на изучение учебной дисциплины отведено:

– для очной формы получения высшего образования – 200 учебных часов, в том числе 72 часа аудиторных занятий, из которых лекционных - 36 часов, лабораторных – 30 часов, управляемая самостоятельная работа (аудиторный контроль) – 6 часов.

Трудоемкость учебной дисциплины составляет 6 зачетных единиц.

Форма промежуточной студентов в рамках данной дисциплины – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Введение

Классификация мобильных приложений. Анализ безопасности мобильных приложений.

Тема 2. Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных. Примеры.

Внутренние и внешние угрозы, классификация вредоносного программного обеспечения. Средства их обнаружения и локализации, описание основных антивирусных программных. Пример разработки «вируса» и соответствующей антивирусной программы

Тема 3. Организационные и правовые аспекты защиты данных.

Основные понятия и определения. Управление, социология, психология, право, организация в защите данных от несанкционированного использования.

Тема 4. Архитектура мобильных приложений.

Эволюция технологий OS X и iOS. Архитектура мобильных приложений iOS-устройств.

Тема 5. Программные и аппаратные средства защиты при разработке мобильных приложений.

Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Аппаратные средства защиты данных. Программные и аппаратные средства защиты данных от копирования. Примеры.

Тема 6. Защита и взлом приложений

Основные способы обеспечения защиты. Методы оценки эффективности защиты. Надежность алгоритмов и протоколов. Актуальные задачи защиты мобильных приложений. Возможности «шифрования данных на аппаратном уровне». Эффективность защиты данных на аппаратном уровне. Причины ослабления средств защиты.

Тема 7. Внутреннее устройство ОС и безопасность

Взлом внутренних процессов ОС и процесса загрузки. Защита ядра и файловой системы iOS.

МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

№п/п	Название темы	Количество часов					Количество часов УСР	Форма контроля знаний
		Аудиторные						
		Лекции	Практ занятия	Сем-занятия	Лаб. занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Введение	2						
2.	Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных. Примеры	4			4			Устный опрос
3.	Организационные и правовые аспекты защиты данных	4					4	Устный опрос
4.	Архитектура мобильных приложений	6			6			Отчет по лабораторной работе
5.	Программные и аппаратные средства защиты при разработке мобильных приложений	8			8		2	Коллоквиум. Отчет по лабораторной работе
6.	Защита и взлом приложений	6			6			Отчет по лабораторной работе
7.	Внутреннее устройство ОС и безопасность	6			6			Контрольная работа. Отчет по лабораторной работе
ИТОГО		36			30		6	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная

1. Вигерс Карл, Битти Джой. Разработка требований к программному обеспечению. 3-е изд. дополненное/ Пер. с англ. – М.: Издательство «Русская редакция»; СПб. :БХВ-Петербург, 2014. – 736 стр.: ил.
2. Ховард М., Лебланк Д. Защищенный код/ Пер. с англ., - 2-е изд, испр. М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 стр.: ил.
3. Ховард М., Лебланк Д., Вьега Дж. 24 смертных греха компьютерной безопасности. Как написать безопасный код / Изд. Питер, 2010. – 400 с.
4. Стив Макконнелл. Совершенный код. Практическое руководство по разработке программного обеспечения. Мастер-класс/ Пер. с англ. – М.: Издательство «Ркссская Редакция»; СПб. : Питер, 2017.
5. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2009.
6. Бурдаев О.В., М.А. Иванов, И.И. Тетерин. Ассемблер в задачах защиты информации. – М.: Кудиц-Образ, 2004.
7. Фленов М. Компьютер глазами хакера. – Санкт-Петербург, БХВ-Петербург, 2012.

Дополнительная

1. Krause M., Tipton H.F. Handbook of information Security Management. – CRC Press LLC. – www.cccure.com
2. The Red Book: A Roadmap for Systems Security Research. Seventh framework programme.- The SysSec Consortium. – www.syssec-project.eu
3. Boran S. IT Security CookBook. – www.boran.com/security
4. Указ Президента Республики Беларусь № 575 от 9 ноября 2010 г. «Об утверждении Концепции национальной безопасности Республики Беларусь. – www.pravo.by

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Объектом диагностики компетенций студентов являются знания, умения, практический опыт, полученные ими в результате изучения учебной дисциплины. Выявление учебных достижений студентов осуществляется с помощью мероприятий текущего контроля и промежуточной аттестации.

Текущий контроль работы студента проходит в следующих формах:

– технические: лабораторные работы, выполняемые на компьютере. Они оцениваются исходя из читаемости и оптимизированности программного кода, а также путём проверки программного кода на тестовых примерах;

– устно-письменные: устная и/или письменная (в виде отчёта) защита лабораторных работ, оцениваемая на основе полноты и последовательности ответа (отчёта), полноты раскрытия содержания выполненного задания, понимания работы алгоритмов и методов, использованных при выполнении задания;

– устные: устные опросы, проводимые в целях первичного мониторинга усвоения материала студентами и оцениваемые исходя из полноты и последовательности ответа, понимания основных понятий, методов и алгоритмов, изложенных на лекционных или лабораторных занятиях; коллоквиум.

Формой промежуточной аттестации по дисциплине «Информационная безопасность мобильных приложений» предусмотрен **экзамен**.

При формировании итоговой отметки используется рейтинговая систе-

ма оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в итоговую отметку:

Формирование отметки за текущую успеваемость:

- устный опрос - 20%,
- отчет по лабораторным работам - 60%,
- коллоквиум - 10%,
- контрольная работа - 10%.

В случае успешной защиты отчётов по всем лабораторным работам, положительных результатов контрольной работы, коллоквиума и устного опроса допускается определение результатов промежуточной аттестации по дисциплине без проведения дополнительного опроса на экзамене. При этом явка обучающегося на экзамен является обязательной.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей успеваемости (рейтинговой системы оценки знаний) и экзаменационной отметки с учетом их весовых коэффициентов. Вес отметки по текущей успеваемости составляет 40%, экзаменационной отметки - 60%

Примерная тематика лабораторных занятий

Лабораторная работа № 1.

Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных.

Лабораторная работа № 2.

Архитектура мобильных приложений.

Лабораторная работа № 3.

Программные средства защиты при разработке мобильных приложений.

Лабораторная работа № 4.

Защита и взлом приложений.

Лабораторная работа № 5.

Внутреннее устройство ОС и безопасность.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются следующие инновационные подходы:

практико-ориентированный подход, который предполагает:

- освоение содержания образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности;
- ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;
- использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

метод проектного обучения, который предполагает:

- способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;
- приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации самостоятельной работы обучающихся

Самостоятельная работа с целью изучения материала учебной дисциплины предполагает работу с рекомендованной учебной литературой и Интернет-ресурсами. Теоретические сведения закрепляются выполнением лабораторных заданий, при выполнении которых следует руководствоваться методическими разработками, размещенными в электронной библиотеке университета и на образовательном портале. Также могут быть предложены дополнительные задания (тесты, задания для самостоятельного выполнения) для самооценки и более глубокого усвоения полученного материала.

Примерный перечень заданий управляемой самостоятельной работы

Тема 3. Организационные и правовые аспекты защиты данных.

Форма контроля – устный опрос

Тема 5. Аппаратные средства защиты при разработке мобильных приложений.

Форма контроля – коллоквиум, отчет по лабораторной работе.

Тематика коллоквиума

Программные и аппаратные средства защиты при разработке мобильных приложений.

Примерный перечень вопросов к экзамену.

1. Архитектура безопасности ОС Linux.
2. Архитектура безопасности ОС macOS.
3. Архитектура безопасности ОС Android.
4. Архитектура безопасности ОС iOS.
5. Архитектура безопасности ОС Windows.
6. Небезопасное программирование (работа со строками, работа с паролями).
7. Контроль доступа в ОС семейства UNIX.
8. Технология User Account Control в Windows.
9. Технология Windows Subsystem for Linux.
10. Технология Windows Subsystem for Android.
11. Технологии и продукты Mobile Device Management, поддержка MDM в Android и iOS.
12. Структура нативного приложения в Android и iOS.
13. Обход механизмов безопасности мобильных ОС. Root и Jailbreak.
14. Категории вредоносного ПО для мобильных ОС.
15. Антивирусные программы для мобильных ОС.
16. Инструменты анализа мобильных приложений
17. Технологии противодействия отладке и обратной разработке.
18. Применение подходов обеспечения ИБ мобильных приложений к IoT-системам.
19. Классификация и оценка рисков. Методологии STRIDE, DREAD.
20. Методология оценки рисков OWASP. Owasp Top 10.
21. OWASP Mobile Top 10 - история, различия между версиями.
22. OWASP MASVS - структура, связь с MSTG и Security Checklist, категории L1, L2, R.
23. OWASP MSTG. Тестирование архитектуры и дизайна (MSTG-ARCH).
24. OWASP MSTG. Тестирование хранения данных (MSTG-STORAGE).
25. OWASP MSTG. Тестирование криптографии (MSTG-CRYPTO).
26. OWASP MSTG. Тестирование аутентификации (MSTG-AUTH).
27. OWASP MSTG. Тестирование сетевого взаимодействия (MSTG-NETWORK).
28. OWASP MSTG. Тестирование взаимодействия с ОС (MSTG-PLATFORM).

29. OWASP MSTG. Тестирование процесса разработки (MSTG-CODE).
30. OWASP MSTG. Тестирование устойчивости к клиентским атакам (MSTG-ARCH).

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Высокоуровневые технологии программирования для компьютерных систем (RFID-технологии)	Технологий программирования	Нет	Оставить содержание учебной дисциплины без изменения, протокол № 16 от 18.05.2023 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры технологий программирования (протокол № ____ от _____ 202_ г.)

Заведующий кафедрой

_____ _____ _____

(учёная степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____

(учёная степень, звание) (подпись) (И.О.Фамилия)