

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЛПУ»)**

Структурное подразделение Институт физико-математического
образования, информационных и обслуживающих технологий
Кафедра информационных образовательных технологий и систем

УТВЕРЖДАЮ

Директор ИФМОИОТ

Е.Е. Горбенко

2023 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Статический анализ программного кода

По направлению подготовки 09.04.04 Программная инженерия

Профиль подготовки Программное обеспечение систем и комплексов

Квалификация выпускника магистр

Форма обучения очная, заочная

Курс ОФО – 2 курс, ЗФО – 2 курс

Луганск, 2023

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы для подготовки магистров по направлению подготовки 09.04.04 Программная инженерия очной и заочной форм обучения.

Рабочая программа учебной дисциплины разработана в соответствии с ФГОС ВО – магистратура по направлению подготовки 09.04.04 «Программная инженерия», утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 No 932 (с изменениями и дополнениями) и Профессиональным стандартом, утвержденным Приказом Министерства труда и социальной защиты Российской Федерации «Об утверждении профессионального стандарта 06.017 «Руководитель разработки программного обеспечения» от 20.07.2022 No 423н.

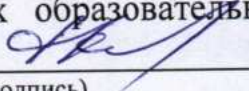
СОСТАВИТЕЛЬ:

доцент кафедры информационных образовательных технологий и систем,
кандидат физико-математических наук, доцент Швыров Вячеслав
Владимирович

Утверждена на заседании кафедры информационных образовательных
технологий и систем

Протокол от «24» ноября 2023 г. №8

Заведующий кафедрой информационных образовательных технологий и
систем

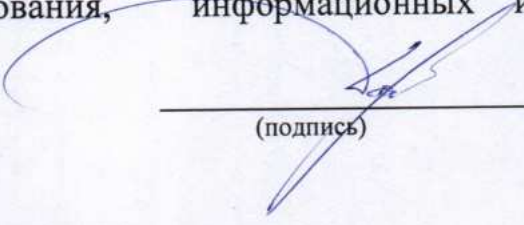

(подпись)

Д.А. Капустин

Одобрена на заседании учебно-методической комиссии Института физико-
математического образования, информационных и обслуживающих
технологий

Протокол от «06» декабря 2023 г. №5

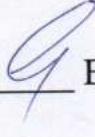
Председатель учебно-методической комиссии Института физико-
математического образования, информационных и обслуживающих
технологий


(подпись)

О.В. Давыскиба

СОГЛАСОВАНО:

Заведующий учебно-методическим отделом


(подпись)

В.В. Савенков

1. Цели и задачи дисциплины

Цели изучения дисциплины: изучение статического анализа потоков данных и его применения для обнаружения дефектов программ, которые могут привести к нарушению безопасности не только рассматриваемой программы, но и всей вычислительной системы, на которой она выполняется.

Задачи:

- формирование профессиональных компетенций, позволяющих выполнять анализ программного кода с целью поиска дефектов и уязвимостей;
- применение современных инструментальных средств для статического анализа кода;
- освоение и применение современных программных комплексов для оценки безопасности программного кода с использованием методов статического анализа.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Статический анализ программного кода» относится к базовой (обязательной) части учебного плана (Б1.О.07). Дисциплина реализуется кафедрой информационных образовательных технологий и систем (4) Институт физико-математического образования, информационных и обслуживающих технологий ФГБОУ ВО «ЛГПУ».

Необходимым условием для освоения учебной дисциплины являются знания основных классов информационных угроз и категорий уязвимостей которые могут быть эффективно обнаружены методами статического анализа; умения пользоваться своими знаниями для повышения качества программного кода, навыки освоения больших объемов информации, представленной в традиционной и электронной форме; навыками грамотной обработки результатов компьютерного моделирования и сопоставления их с теоретическими данными; практикой исследования и решения теоретических и прикладных задач; навыками теоретического анализа реальных задач, связанных с представлением и обработкой знаний.

Содержание дисциплины «Статический анализ программного кода» является логическим продолжением содержания дисциплин «Технология разработки программного обеспечения» и основой для дальнейшего освоения дисциплин: «Исследование и проектирование систем искусственного интеллекта», написания магистерской диссертации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код по ФГОС ВО	Индикатор достижения	Результаты обучения по дисциплине
Универсальные		
Общепрофессиональные		

ОПК-8. Способен осуществлять эффективное управление разработкой программных средств и проектов	ОПК-8.1. Знать методы эффективного управления разработкой программных средств и проектов ОПК-8.2. Уметь применять эффективное управление разработкой программных средств и проектов ОПК-8.3. Владеть навыками эффективного управления разработкой программных средств и проектов	ОПК-8.1. Знает методы эффективного управления разработкой программных средств и проектов ОПК-8.2. Умеет применять эффективное управление разработкой программных средств и проектов ОПК-8.3. Владеет навыками эффективного управления разработкой программных средств и проектов
Профессиональные		
ПК-1. Знание методов организации и управления информационными процессами	ПК-1.1. Знать методы управления информационными процессами ПК-1.2. Уметь управлять проектами по информатизации предприятий ПК-1.3. Владеть навыками практического управления проектами по информатизации предприятий	ПК-1.1. Знает методы управления информационными процессами ПК-1.2. Умеет управлять проектами по информатизации предприятий ПК-1.3. Владеет навыками практического управления проектами по информатизации предприятий проектных решений

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (4 зач. ед.)	
	Очная форма	Заочная форма
Общая учебная нагрузка (всего)	144	144
Обязательная аудиторная учебная нагрузка (всего часов), в том числе:		
Лекции	16	6
Семинарские занятия		
Практические занятия		
Лабораторные работы	32	10
Курсовая работа / курсовой проект		
Другие формы организации учебного процесса (контрольные работы, индивидуальные занятия, консультации и др.)	27	9
Самостоятельная работа студента (всего)	69	9
Форма аттестация	Экзамен	Экзамен

4.2. Содержание дисциплины

Тема 1. Введение. Проблема безопасности ПО и статический анализ.

Проблема безопасности ПО как проблема программной инженерии. Необходимость выявления дефектов ПО (в частности, уязвимостей и ошибок в работе с динамической памятью). Возможности статического анализа по решению проблем безопасности.

Тема 2. Применение статического анализа для обнаружения потенциальных угроз. Категории уязвимостей

Методы применения статического анализа для выявления уязвимостей в коде. Основные категории уязвимостей, такие как инъекции, недостатки аутентификации и авторизации, межсайтовый скриптинг и другие. Роль статического анализа в повышении безопасности программного обеспечения. Эффективные инструменты статического анализа для выявления угроз безопасности.

Тема 3. Автоматизированные инструменты статического анализа.

Методы автоматизированного статического анализа для различных языков. Особенности, синтаксические деревья кода

Тема 4. Статический анализ для различных языков программирования.

Общие методы и подходы выполнения статического анализа для различных языков. Повышение качества кода. Рефакторинг кода.

Тема 5. Особенности статического анализа программ на Python.

Особенности языка Python. Особенности статического анализа для языка Python. Основные сложности языков с динамической типизацией

Тема 6. Статический анализ проектов на C#.

Особенности статического анализа кода на языке C#. Современные средства проверки кода для языка C#

Тема 7. Каталог CWE и БДУ.

Структура каталогов CWE и БДУ. Новый раздел в БДУ. Особенности поиска уязвимостей. Получение данных в JSON

Тема 8. Методы устранения дефектов в коде.

Особенности устранения различных видов дефектов в программном коде.

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
3 семестр / 4-5 триместр			
1	Тема 1. Введение. Проблема безопасности ПО и статический анализ.	2	2
2	Тема 2. Применение статического анализа для обнаружения потенциальных угроз. Категории уязвимостей	2	2
3	Тема 3. Автоматизированные инструменты статического анализа.	2	2
4	Тема 4. Статический анализ для различных языков программирования.	2	

5	Тема 5. Особенности статического анализа программ на Python.	2	
6	Тема 6. Статический анализ проектов на C#.	2	
7	Тема 7. Каталог CWE и БДУ.	2	
8	Тема 8. Методы устранения дефектов в коде.	2	
Итого:		16	6

4.4. Практические занятия

Не предусмотрено учебным планом

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
3 семестр / 4-5 триместр			
1	Установка Anaconda. Управление пакетами и окружениями	4	2
2	Основы синтаксиса Python. PEP 8	2	2
3	Современные линтеры. Работа с flake	2	2
4	Работа с Bandit	2	2
5	Работа с Black	2	2
6	Автокорректировщики кода. YAPF	2	
7	Проверка импортируемых библиотек и зависимостей в проектах	2	
8	Статический анализ кода на C#	2	
9	Создание анализатора на основе шаблонов Visual Studio	2	
10	Нейросетевой детекторы ошибок	2	
11	Изучение веб-приложений для анализа кода. Snyk	2	
12	Безопасность проектов размещенных на GitHub	2	
13	Выявление устаревших и слабых криптоалгоритмов в коде	2	
14	Детектирование командных инъекций	2	
15	Разработка собственного статического анализатора	2	
Итого:		32	10

4.6. Самостоятельная работа студентов

№ п/п	Название раздела / темы	Вид самостоятельной работы	Объем часов	
			Очная форма	Заочная форма
3 семестр / 4-5 триместр				
1	Оптимизация кода через статический анализ	Конспект лекций	14	2
2	Интеграция статического анализа в CI/CD конвейер	Конспект лекций	14	2
3	Анализ безопасности с	Конспект лекций	14	2

	использованием статического анализа			
4	Исследование инструментов статического анализа	Конспект лекций	14	2
5	Статический анализ в реальном проекте	Конспект лекций	13	1
Итого:			69	9

4.7. Курсовые работы / проекты

5. Методическое обеспечение, образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий.

Наряду с методикой традиционной лекционно-практической работы предусмотрено использование активных форм и методов учебной деятельности, в том числе: учебные дискуссии, беседы, мозговой штурм.

Методика проблемно-диалогического обучения применяется в процессе лекционной работы над учебным материалом в каждой из тем учебной дисциплины.

Методика обучения в сотрудничестве с применением командных, групповых видов работы используется в процессе организации лабораторных работ.

Методика исследовательской деятельности используется как основа для организации самостоятельной работы студентов в объеме учебных тем. Применяются средства мультимедиа: презентации, видео, базы ЭОР.

Информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный во внутренней сети или т.п.) при подготовке к лекциям, лабораторным работам и самостоятельной работе.

Работа в команде, проектная деятельность: совместная работа студентов в группе при выполнении лабораторных работ.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы в следующих формах: выполнение лабораторных работ; защита лабораторных работ.

Промежуточный контроль по результатам освоения дисциплины проходит в форме зачета (включает в себя ответ на теоретические вопросы и выполнение тестового задания).

Система оценивания учебных достижений студентов, оценочные средства представлены в фонде оценочных средств к рабочей программе учебной дисциплины (в приложении).

7. Учебно-методическое и программно-информационное обеспечение дисциплины

А) основная литература:

1. Бэрри П. Изучаем программирование на Python. - М., 2017. - 624 с.
2. Буйначев С. К. Основы программирования на языке Python: учебное пособие. - Екатеринбург: Изд-во Урал. ун-та, 2014. - 91 с.
3. Бхаргава А. Грожаем алгоритмы: иллюстрированное пособие для программистов и любопытствующих. - СПб.: Питер, 2017. - 288 с.
4. Гэддис Т. Начинаем программировать на Python / пер. с англ. 4-е изд. - СПб.: БХВ-Петербург, 2019. - 768 с.
5. Мюллер Дж. Python для чайников. - СПб. : Диалектика, 2019. - 416 с.

Б) дополнительная литература:

1. Лутц М. Изучаем Python, пер. с англ. 3-е изд. - СПб.: Символ Плюс, 2009. - 848 с.
2. Brian Chess and Jacob West. Secure Programming with Static Analysis. Pearson Education, Inc. 2007, ISBN: 0-321-42477-8.
3. Рейтц К., Шлюссер Т. Автостопом по Python. - СПб. : Питер, 2017. - 336 с.
4. Фёдоров Д. Ю. Программирование на языке высокого уровня Python: учебное пособие для прикладного бакалавриата. - М. : Издательство Юрайт, 2019. - 161 с.

В) Интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины

Лекционные занятия: комплект электронных презентаций/слайдов, аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и т.п.

Лабораторные работы: компьютерный класс, оснащенный мультимедийным проектором, интерактивной доской, сетевой инфраструктурой и организованным доступом в Интернет, пакеты ПО MS Word, MS Excel, Anaconda, редактор Spider, пакеты Flake, Bandit, Yarpf. Visual Studio..

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде и т.п.

9. Лист дополнений и изменений

[illegible]