

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»**

Радиофизический факультет

(факультет / институт / филиал)

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«20» апреля 2021г. № 1

Рабочая программа дисциплины

Методы оценки безопасности программного кода

(наименование дисциплины (модуля))

Уровень высшего образования

специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

10.05.02 Информационная безопасность телекоммуникационных систем

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2021 год

1. Место дисциплины в структуре ООП

Дисциплина «Методы оценки безопасности программного кода» относится к части, формируемой участниками образовательных отношений, основной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
2	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.ДВ.03.01 «Методы оценки безопасности программного кода» относится к части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», формируемой участниками образовательных отношений.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
ПК-2. Способен анализировать угрозы информационной безопасности цифровых телекоммуникационных сетей, контролировать их работоспособность и оценивать эффективность	ПК-2.1. Знает: - методы создания моделей угроз информационной безопасности цифровых телекоммуникационных сетей - методики оценки уязвимостей цифровых телекоммуникационных сетей с точки зрения возможности НСД к ним	Знать: - общие свойства и взаимозависимости различных видов моделей программных объектов - методики оценки уязвимостей операционных систем с точки зрения возможности НСД к ним	Собеседование
	ПК-2.2. Умеет: - разрабатывать модели угроз, и систематизировать сведения об угрозах информационной безопасности	Уметь: - определять параметры моделей программных систем - оценивать и анализировать основные характеристики функциональных частей операционных систем	Собеседование

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	2 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	72		
в том числе			
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа (практические занятия / лабораторные работы)	32		
самостоятельная работа	39		
КСР	1		
Промежуточная аттестация – экзамен/зачет	зачет		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего (часы)	В том числе				
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Методы анализа исходного программного кода	5	2			2	3
2. Статические методы анализа безопасности программного обеспечения	12	6			6	6
3. Динамические методы анализа	12	6			6	6

безопасности программного обеспечения						
4. Сигнатурно-эвристический анализ исходного и выполняемого кода	5	2			2	3
5. Структурный анализ избыточности дистрибутива и контроль над целостностью	6	2			2	4
6. Анализ подсистем безопасности	8	4			4	4
7. Анализ наличия скрытых каналов	5	2			2	3
8. Методы доказательства правильности программ и их спецификаций	9	4			4	5
9. Функциональное, стрессовое, нагрузочное тестирование и тестирование производительности	9	4			4	5
Итого:	71	32			32	39

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:

- изучение дополнительных разделов дисциплины с использованием учебной литературы.

Текущий контроль усвоения материала проводится путем проведения опроса.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций	
	не зачтено	зачтено

<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения, . Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка	Уровень подготовки
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»

	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1 Контрольные вопросы

<i>Вопросы</i>	<i>Код формируемой компетенции</i>
1. Проверка кода без его выполнения.	ПК-2
2. Проверка поведения программы без сканирования исходного кода.	ПК-2
3. Проверка архитектуры и логики	ПК-2
4. Сколько уровней контроля на отсутствие недекларируемых возможностей устанавливает РД НДВ?	ПК-2
5. Какие испытания включает в себя статический анализ?	ПК-2
6. Какие испытания включает в себя динамический анализ?	ПК-2
7. Приведите примеры программ для проведения статического, динамического анализа.	ПК-2
8. Ошибки какого типа могут быть выявлены с помощью фаззинга?	ПК-2
9. Какие типы фаззинга существуют?	ПК-2
10. Какой метод позволяет увеличить покрытие тестируемой программы при наличии ее исходных текстов?	ПК-2
11. Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность программ.	ПК-2
12. Модель угроз и принципы обеспечения безопасности программного обеспечения.	ПК-2
13. Формальные методы доказательства правильности программ и их спецификаций.	ПК-2
14. Методы и средства анализа безопасности программного обеспечения.	ПК-2
15. Методы обеспечения надежности программ для контроля их технологической безопасности.	ПК-2
16. Методы создания алгоритмически безопасных процедур.	ПК-2
17. Методы идентификации программ и их характеристик.	ПК-2
18. Методы и средства защиты программ от компьютерных вирусов.	ПК-2
19. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок.	ПК-2
20. Методы и средства обеспечения целостности и достоверности используемого программного кода.	ПК-2
21. Основные подходы к защите программ от несанкционированного копирования.	ПК-2

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Дастин Э., Рэшке Д., Пол Д. Автоматизированное тестирование программного обеспечения: внедрение, управление, эксплуатация. -М.: Лори, 2003.
2. Герасименко В.А. Защита информации в АСОД.- М.: Энергоиздат, 1994.
3. Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей. - Учеб пособие. - СПб: Издательство ВИКА им. А.Ф. Можайского, 1997.
4. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. - СПб.: Наука, 1994.
5. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под. ред. А.С.Маркова. -М.:Радио и связь, 2012. 192 с.

б) дополнительная литература:

1. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. - М.: Гостехкомиссия России, 1998.
2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: ИПК «Изд-во стандартов», 2002.
3. ГОСТ РВ 51719-2001. Испытания программной продукции. - М.: ИПК «Изд-во стандартов», 2001.
4. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: Гостехкомиссия России, 2002
5. Абрамов С.А. Элементы анализа программ. Частичные функции на множестве состояний. - М.: Наука, 1986.
6. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. .. Мир, 1979.
7. Марков А.С., Фадин А.А. Статический сигнатурный анализ безопасности программ/ Программная инженерия и информационная безопасность. 2013. № 1. С. 50-56.
8. Стельмашонок Е.В. Моделирование процессов и систем. – М.: Издательство Юрайт, 2017. – 289 с. [Электронный ресурс: <https://biblio-online.ru/book/68D5E3CE-5293-4F66-9C33-1F6CF0A2D5F2>]
9. Анализ данных / под ред. В.С. Мхитаряна. – М.: Издательство Юрайт, 2017. – 490 с. [Электронный ресурс: <https://biblio-online.ru/book/CC38E97A-CCE5-4470-90F1-3B6D35ACC0B4>]

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ Л.Ю. Ротков

_____ А.А. Горбунов

Заведующий кафедрой «Безопасность
информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «23» марта 2021 года, протокол № 02/21.