Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы»

Инженерная академия

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

27.04.04 УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

АНАЛИЗ БОЛЬШИХ ДАННЫХ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Анализ уязвимостей программного обеспечения» входит в программу магистратуры «Анализ больших данных и технологии защиты информации» по направлению 27.04.04 «Управление в технических системах» и изучается в 1 семестре 1 курса. Дисциплину реализует Кафедра механики и процессов управления. Дисциплина состоит из 5 разделов и 18 тем и направлена на изучение методов анализа уязвимостей программного обеспечения, используемых при решении задач анализа алгоритмов защиты информации, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

Целью освоения дисциплины является приобретение практических навыков выявления уязвимостей в программных реализациях, устранение выявленных уязвимостей, использование теории выявления слабых мест при проведении сертификационных испытаний применительно к задачам, связанным с защитой информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Анализ уязвимостей программного обеспечения» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	**Компетенция**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
ОПК-5	Способен проводить патентные исследования, определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности, распоряжаться правами на них для решения задач в развития науки, техники и технологии	ОПК-5.1 Знает методы и подходы к проведению патентных исследований, формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности;; ОПК-5.2 Умеет распоряжаться правами на результаты интеллектуальной деятельности для решения задач в области развития науки, техники и технологии;; ОПК-5.3 Владеет методами и подходами к проведению патентных исследований, знает методы правовой охраны и защиты прав на результаты интеллектуальной деятельности.;
ОПК-6	Способен осуществлять сбор и проводить анализ научно-технической информации, обобщать отечественный и зарубежный опыт в области средств автоматизации и управления	ОПК-6.1 Знает основные методы сбора и проведения анализа научно-технической информации;; ОПК-6.2 Умеет анализировать и обобщать отечественный и зарубежный опыт в области средств автоматизации и управления;; ОПК-6.3 Владеет методами сбора и проведения анализа научно-технической информации, а также может обобщать отечественный и зарубежный опыт в профессиональной отрасли.;
ОПК-8	Способен выбирать методы и разрабатывать системы управления сложными техническими объектами и технологическими процессами	ОПК-8.1 Знает основные методы, применяемые для разработки систем управления сложными техническими объектами и технологическими процессами;; ОПК-8.2 Умеет разрабатывать системы управления сложными техническими объектами и технологическими процессами;; ОПК-8.3 Имеет навыки выбора методов и разработки систем управления сложными техническими объектами и технологическими процессами.;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Анализ уязвимостей программного обеспечения» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Анализ уязвимостей программного обеспечения».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
ОПК-6	Способен осуществлять сбор и проводить анализ научно-технической информации, обобщать отечественный и зарубежный опыт в области средств автоматизации и управления		Преддипломная практика;
ОПК-5	Способен проводить патентные исследования, определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности, распоряжаться правами на них для решения задач в развития науки, техники и технологии		Научно-исследовательская работа; Преддипломная практика;
ОПК-8	Способен выбирать методы и разрабатывать системы управления сложными техническими объектами и технологическими процессами		Научно-исследовательская работа; Преддипломная практика; Защищенное программное обеспечение; Динамика и управление космическими системами;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Анализ уязвимостей программного обеспечения» составляет «6» зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			1
Контактная работа, ак.ч.	*68*		*68*
Лекции (**ЛК**)	34		34
Лабораторные работы (**ЛР**)	34		34
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*121*		*121*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***216***	*216*
	зач.ед.	***6***	*6*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Введение	1.1	Основные виды и наиболее известные примеры программных уязвимостей.	ЛК, ЛР
		1.2	Основные средства и методы анализа программных реализаций на предмет уязвимостей	ЛК, ЛР
Раздел 2	Защита информации с использованием шифровальных (криптографических) средств	2.1	Криптографические методы защиты информации.	ЛК, ЛР
		2.2	Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.	ЛК, ЛР
Раздел 3	Комплексная защита объектов информатизации	3.1	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).	ЛК, ЛР
		3.2	Администрирование сертифицированных защищенных операционных систем.	ЛК, ЛР
		3.3	Механизмы безопасности сертифицированных защищенных операционных систем.	ЛК, ЛР
Раздел 4	Проведение экспертизы качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности	4.1	Выявления уязвимостей в программных реализациях.	ЛК, ЛР
		4.2	Устранение выявленных уязвимостей в программных реализациях.	ЛК, ЛР
Раздел 5	Методология проведения анализа уязвимости	5.1	Разработка методики проведения анализа уязвимости объекта оценки.	ЛК, ЛР
		5.2	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «Cross Site Scripting».	ЛК, ЛР
		5.3	Практика выявления уязвимостей класса «Cross Site Scripting» при проведении сертификационных испытаний.	ЛК, ЛР
		5.4	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «Cross Site Request Forgery».	ЛК, ЛР
		5.5	Практика выявления уязвимостей класса «Cross Site Request Forgery» при проведении сертификационных испытаний.	ЛК, ЛР
		5.6	Практика выявления уязвимостей класса «Переполнение буфера» при проведении сертификационных испытаний.	ЛК, ЛР
		5.7	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «SQL Injection».	ЛК, ЛР
		5.8	Практика выявления уязвимостей класса «SQL Injection» при проведении сертификационных испытаний.	ЛК, ЛР
		5.9	Отчетность по результатам проведения анализа уязвимости в рамках сертификационных испытаний.	ЛК, ЛР

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.*

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве [Параметр] шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Запечников, С. В. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с.

2. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. Часть 1 и 2. — М.: издательство Юрайт, 2017.

3. Tanja Lange • Tsuyoshi Takagi (Eds.). Post-Quantum Cryptography. 8th International Workshop, PQCrypto 2017. Springer. 2017. – 429с.

4. Ховард М. Уязвимости в программном коде и борьба с ними. ДМК Пресс, 2011, 288с.

5. Л.К. Бабенко, Е.А. Ищукова Криптографические методы и средства обеспечения информационной безопасности, 2011.

Дополнительная литература:

1. Долозов Н. Л. Программные средства защиты информации / Н.Л. Долозов; Т.А. Гультяева - Новосибирск: НГТУ, 2015. - 63 с.

2. Прохорова О. В. Информационная безопасность и защита информации / О.В. Прохорова - Самара: Самарский государственный архитектурно-строительный университет, 2014. -113 с.

3. Руденков Н. А. Технологии защиты информации в компьютерных сетях / Н.А. Руденков - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. Электронный ресурс

4. С.П. Вартанов, А.Ю. Герасимов. Динамический анализ программ с целью поиска ошибок и уязвимостей при помощи целенаправленной генерации входных данных. Труды ИСП РАН том 26 вып. 1, 2014. С. 375-394.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН http://lib.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС Юрайт http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Анализ уязвимостей программного обеспечения».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

РАЗРАБОТЧИК:

Доцент		Велигура Александр Николаевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Разумный Юрий Николаевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Профессор		Разумный Юрий Николаевич
Должность, БУП	*Подпись*	*Фамилия И.О.*