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)

2026 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 развитии 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 развитии науки, техники и технологии		Научно-исследовательская работа; Преддипломная практика;
ОПК-8	Способен выбирать методы и разрабатывать системы управления сложными техническими объектами и технологическими процессами		Защищенное программное обеспечение; Динамика и управление космическими системами; Научно-исследовательская работа; Преддипломная практика;

* - 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	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Введение	1.1	Основные виды и наиболее известные примеры программных уязвимостей.	Классификация программных управленческих задач в области информационной безопасности. Задачи управления уязвимостями, управления доступом, управления событиями безопасности и реагирования на инциденты. Наиболее известные примеры: управление идентификацией и доступом Identity and Access Management, управление событиями и информацией безопасности Security Information and Event Management, управление уязвимостями Vulnerability Management. Типовые сценарии использования программных средств в управлении защитой информации.	ЛК, ЛР
		1.2	Основные средства и методы анализа программных реализаций на предмет уязвимостей	Классификация средств анализа программных реализаций. Статические анализаторы кода для исследования исходного текста программ. Динамические анализаторы для наблюдения за поведением программы во время выполнения. Инструменты фаззинга для автоматизированного поиска ошибок обработки входных данных. Сканеры уязвимостей для обнаружения известных уязвимостей. Методы анализа: анализ потока данных, анализ потока управления, символьное выполнение. Сравнительная характеристика автоматизированных и ручных методов анализа. Анализ исходного кода и бинарного кода.	ЛК, ЛР
Раздел 2	Защита информации с использованием шифровальных (криптографических) средств	2.1	Криптографические методы защиты информации.	Основные криптографические методы защиты информации от уязвимостей. Шифрование симметричное с использованием одного секретного ключа. Шифрование асимметричное с использованием пары открытого и закрытого ключей. Хеширование для контроля целостности данных. Электронная подпись для обеспечения аутентичности и неотказуемости. Области применения криптографических методов: защита каналов связи, защита хранилищ данных, защита от несанкционированного доступа.	ЛК, ЛР
		2.2	Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.	Понятие электронной подписи как средства подтверждения подлинности электронного документа. Инфраструктура открытого ключа Public Key Infrastructure, PKI. Состав PKI: удостоверяющие центры, регистрационные центры, центры	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				управления ключами. Сертификаты открытого ключа и их жизненный цикл: создание, распространение, хранение, отзыв. Сертифицированные средства электронной подписи. Интеграция PKI в корпоративные информационные системы для защиты от уязвимостей, связанных с подменой отправителя.	
Раздел 3	Комплексная защита объектов информатизации	3.1	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).	Нормативно-правовая база защиты персональных данных. Классы информационных систем персональных данных ИСПДН в зависимости от уровня защищённости. Организационные меры защиты: назначение ответственных, обучение персонала, контроль доступа. Технические меры защиты: средства антивирусной защиты, средства анализа уязвимостей, средства обнаружения вторжений. Аттестация объектов информатизации и ввод в эксплуатацию. Ответственность за нарушения безопасности персональных данных.	ЛК, ЛР
		3.2	Администрирование сертифицированных защищенных операционных систем.	Понятие сертифицированной защищённой операционной системы. Порядок сертификации операционных систем по требованиям безопасности информации. Основные задачи администрирования: управление учётными записями пользователей, назначение прав доступа к ресурсам, настройка политик безопасности. Аудит событий безопасности для выявления признаков атак. Конфигурирование механизмов контроля доступа: дискреционного и мандатного. Установка обновлений безопасности и управление уязвимостями операционной системы.	ЛК, ЛР
		3.3	Механизмы безопасности сертифицированных защищенных операционных систем.	Классификация механизмов безопасности защищённых операционных систем. Идентификация и аутентификация пользователей. Регистрация событий безопасности с ведением журналов аудита. Контроль целостности системных файлов и конфигураций. Разграничение доступа к объектам файловой системы и процессам. Защита от несанкционированного доступа к памяти и привилегированным режимам выполнения. Механизмы изоляции процессов и приложений.	ЛК, ЛР
Раздел 4	Проведение экспертизы качества и надежности	4.1	Выявления уязвимостей в программных реализациях.	Методы обнаружения уязвимостей в программном обеспечении. Классификация уязвимостей по природе	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
	программных и программно-аппаратных средств обеспечения информационной безопасности			возникновения: ошибки ввода-вывода, ошибки управления памятью, ошибки авторизации и аутентификации. Приоритизация выявленных уязвимостей по степени критичности и вероятности эксплуатации. Использование общедоступных баз уязвимостей, включая Common Vulnerabilities and Exposures CVE и Common Vulnerability Scoring System CVSS. Документирование выявленных уязвимостей для последующего устранения.	
		4.2	Устранение выявленных уязвимостей в программных реализациях.	Методы исправления уязвимостей в программном коде. Выпуск и применение обновлений безопасности патчей. Контроль эффективности устранения уязвимостей с помощью повторного тестирования. Реализация защитных механизмов на уровне прикладного программного обеспечения. Мониторинг появления новых уязвимостей в используемых компонентах после устранения.	ЛК, ЛР
Раздел 5	Методология проведения анализа уязвимости	5.1	Разработка методики проведения анализа уязвимости объекта оценки.	Принципы построения методики анализа уязвимостей для сертификационных испытаний. Определение целей и задач анализа. Выбор инструментальных средств тестирования. Установление критериев выявления уязвимостей. Формирование процедур проведения анализа. Разработка шаблонов отчётной документации по результатам испытаний.	ЛК, ЛР
		5.2	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «Cross Site Scripting».	Понятие атак класса Cross Site Scripting XSS. Механизмы возникновения уязвимости при некорректной обработке пользовательского ввода. Типы XSS: отражённая Reflected XSS, сохранённая Stored XSS, DOM-основанная DOM-based XSS. Потенциальные последствия эксплуатации XSS-уязвимостей: кража сессий, подмена содержимого страниц, перенаправление на вредоносные сайты. Способы защиты: экранирование вывода, фильтрация ввода, использование политики безопасности содержимого Content Security Policy.	ЛК, ЛР
		5.3	Практика выявления уязвимостей класса «Cross Site Scripting» при проведении сертификационных испытаний.	Методика практического тестирования на наличие XSS-уязвимостей. Использование тестовых полезных нагрузок payloads для обнаружения отражённого и сохранённого XSS. Ручное тестирование полей ввода веб-форм и параметров URL. Применение автоматизированных сканеров безопасности для обнаружения XSS. Анализ ответов сервера на наличие	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				неэкранированного исполняемого кода. Фиксация доказательств обнаружения уязвимости.	
		5.4	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «Cross Site Request Forgery».	Понятие атак класса Cross Site Request Forgery CSRF. Механизм эксплуатации CSRF-уязвимостей: принуждение аутентифицированного пользователя к выполнению нежелательных действий. Отличие CSRF от XSS. Условия возникновения CSRF-уязвимостей: отсутствие уникальных токенов запроса, предсказуемость параметров запроса. Последствия эксплуатации: изменение пароля, совершение финансовых операций, удаление данных. Способы защиты: использование анти-CSRF токенов, проверка заголовка Referer, повторная аутентификация для критических операций.	ЛК, ЛР
		5.5	Практика выявления уязвимостей класса «Cross Site Request Forgery» при проведении сертификационных испытаний.	Методика практического обнаружения CSRF-уязвимостей. Анализ веб-приложений на предмет отсутствия защитных механизмов. Создание поддельных запросов с использованием HTML-форм и JavaScript. Проверка возможности выполнения критических операций без знания токена пользователя. Тестирование защиты на основе уникальных маркеров сессии. Документирование условий успешной эксплуатации CSRF-уязвимости.	ЛК, ЛР
		5.6	Практика выявления уязвимостей класса «Переполнение буфера» при проведении сертификационных испытаний.	Понятие уязвимости переполнения буфера. Механизм эксплуатации: запись данных за пределами выделенной области памяти. Причины возникновения: отсутствие проверки границ буфера при операциях копирования и ввода. Последствия эксплуатации: отказ в обслуживании, выполнение произвольного кода, повышение привилегий. Практические методы выявления: фаззинг с генерацией некорректных входных данных, статический анализ кода, динамический анализ с использованием отладчиков. Способы защиты: канарейки стека, рандомизация адресного пространства ASLR, предотвращение выполнения кода в стеке DEP.	ЛК, ЛР
		5.7	Теория выявления слабых мест при проведении сертификационных испытаний в механизмах защиты от атак класса «SQL Injection».	Понятие атак класса SQL Injection. Механизм возникновения уязвимости при формировании SQL-запросов с нефильтрованным пользовательским вводом. Типы SQL-инъекций: классическая, слепая Boolean-based blind SQL injection, временная Time-based blind SQL injection,	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				внеканальная Out-of-band SQL injection. Последствия эксплуатации: несанкционированное чтение данных, модификация данных, выполнение административных операций в базе данных, в некоторых случаях выполнение команд на сервере. Способы защиты: параметризованные запросы, экранирование специальных символов, минимальные привилегии учётной записи базы данных.	
		5.8	Практика выявления уязвимостей класса «SQL Injection» при проведении сертификационных испытаний.	Методика практического обнаружения SQL-инъекций. Тестирование полей ввода и параметров URL с использованием специальных символов и синтаксических конструкций SQL. Обнаружение признаков уязвимости по сообщениям об ошибках базы данных. Использование методов слепого внедрения Blind SQL Injection для извлечения данных при отсутствии вывода ошибок. Применение автоматизированных инструментов: sqlmap, специализированных сканеров безопасности. Фиксация доказательств успешного внедрения и извлечения данных. Документирование обнаруженных SQL-инъекций в отчёте.	ЛК, ЛР
		5.9	Отчетность по результатам проведения анализа уязвимости в рамках сертификационных испытаний.	Состав и структура отчётной документации по итогам анализа уязвимостей. Формирование перечня обнаруженных уязвимостей с указанием класса критичности. Описание условий эксплуатации каждой уязвимости. Предоставление доказательств в виде скриншотов, логов, сетевых дампов. Разработка рекомендаций по устранению выявленных уязвимостей. Оформление заключения о соответствии объекта оценки требованиям безопасности. Порядок передачи отчётности в сертификационные органы и заказчику.	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 ____ 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 https://mega.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 «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

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.*