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

Факультет физико-математических и естественных наук

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИСТОЧНИКИ УГРОЗ КИБЕРБЕЗОПАСНОСТИ И АНАЛИЗ УЯЗВИМОСТЕЙ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.04.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

(код и наименование направления подготовки/специальности)

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

БЕСПРОВОДНЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ И КИБЕРБЕЗОПАСНОСТЬ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Источники угроз кибербезопасности и анализ уязвимостей» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается в 1 семестре 1 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 4 разделов и 17 тем и направлена на изучение нормативно-правовых и организационных основ анализа уязвимостей в Российской Федерации и международной практике; освоение классификаций источников угроз и типов угроз кибербезопасности согласно стандартам NIST, ФСТЭК России, ENISA; формирование навыков работы с базами данных уязвимостей (CVE, CWE, NVD) и средствами их обнаружения; освоение методологий оценки критичности и приоритизации уязвимостей (CVSS, EPSS, CISA SSVC); Развитие практических компетенций по идентификации, анализу и оценке уязвимостей в информационных системах.

Целью освоения дисциплины является формирование у обучающихся системных компетенций в области нормативно-правового регулирования, классификации источников угроз, анализа и оценки уязвимостей информационных систем с применением международных и национальных стандартов, методологий и специализированных инструментов.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Источники угроз кибербезопасности и анализ уязвимостей» 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-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1 Определяет информационно-коммуникационные технологии, необходимые для решения задач в области профессиональной деятельности; ОПК-4.2 Оценивает риски и угрозы при использовании информационно-коммуникационных технологий, определяет способы и инструменты защиты данных при решении задач в области профессиональной деятельности; ОПК-4.3 Применяет на практике методы и средства защиты информации при ее сборе, хранении, обработке и передаче;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Источники угроз кибербезопасности и анализ уязвимостей» 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 «Источники угроз кибербезопасности и анализ уязвимостей».

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-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности		Научно-исследовательская работа; Криптографические методы защиты информации; Анализ и показатели эффективности кибербезопасности предприятия;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Источники угроз кибербезопасности и анализ уязвимостей» составляет «4» зачетные единицы.

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.	*36*		*36*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	18		18
Самостоятельная работа обучающихся, ак.ч.	*81*		*81*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

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	Нормативно-правовые и организационные основы анализа уязвимостей.	1.1	Основные понятия и термины	Понятие анализа уязвимостей. Цели и задачи анализа уязвимостей. Этапы процесса анализа уязвимостей (Vulnerability Management). Основные термины в кибербезопасности. Связь понятий: слабое место, уязвимость, угроза, риск. Угрозы и инциденты в киберпространстве. Критическая информационная инфраструктура (КИИ).	ЛК, СЗ
		1.2	Понятие Vulnerability Analysis (анализ уязвимостей) в международных стандартах	Анализ уязвимостей в контексте стандартов. Стандарт проведения тестирования на проникновение (PTES). NIST SP 800-30. ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408 - критерии оценки безопасности ИТ. Значимость уязвимостей (ГОСТ Р ИСО/МЭК 15408-3-2013, п. 5.2.1). ГОСТ Р ИСО/МЭК 15408-3-2013. Причины уязвимостей (п. 5.2.2). Анализ уязвимостей в рамках оценки доверия. ISO/IEC TR 20004:2015. SO/IEC 18045 - методология оценки безопасности ИТ. Основные документы по анализу уязвимостей ФСТЭК России.	ЛК, СЗ
		1.3	Базы данных и информационные ресурсы об уязвимостях	Роль информационных ресурсов в анализе уязвимостей. Международные базы данных: CVE и NVD. CWE и CVSS - классификация и оценка уязвимостей. Exploit Database и SANS Vulnerability Summaries. OSV - уязвимости в open-source программном обеспечении. Банк данных угроз ФСТЭК России (БДУ). Национальный координационный центр по компьютерным инцидентам (НКЦКИ).	ЛК, СЗ
		1.4	Средства обнаружения и анализа уязвимостей	Роль автоматизированных средств в анализе уязвимостей. Сетевые сканеры: Nmap, Masscan, Angry IP Scanner. Сканеры уязвимостей: функции и особенности. Зарубежные и российские инструменты. Ограничения и риски при использовании сканеров. Рекомендации по использованию сканеров.	ЛК, СЗ
Раздел 2	Классификация источников угроз	2.1	Источники угроз в стандартах американского национального института стандартов и технологий (NIST)	Определение источника угрозы в международных стандартах. Подход NIST (США). Классификация источников угроз: российский подход. Антропогенные источники угроз. Техногенные источники угроз. Стихийные источники угроз. Сравнение подходов: NIST и РФ. Практическое значение	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				классификации. Взаимосвязь угроз, уязвимостей и риск.	
		2.2	Выписка из методики оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021)	Назначение методики оценки угроз безопасности информации ФСТЭК России. Разработка отраслевых и корпоративных методик. Определение источников угроз безопасности информации по методике ФСТЭК России. Актуальные нарушители: категории и досту. Категории нарушителей. Уровни возможностей нарушителей. Включение техногенных источников в модель угроз. Основные факторы техногенных угроз. Методы определения вероятности реализации техногенных угроз. Исходные данные для идентификации источников угроз. Практическое значение классификации.	ЛК, СЗ
		2.3	Источники угроз в NIST SP 800-30 Guide for Conducting Risk Assessments	Процесс оценки рисков в информационной безопасности. Методология оценки рисков. Способ анализа рисков. Модель риска и её основные факторы. Классификация источников угроз.	ЛК, СЗ
Раздел 3	Классификация угроз кибербезопасности	3.1	Классификация возникающих угроз в базовой модели угроз безопасности ПДн при их обработке в ИС персональных данных (ФСТЭК России)	Нормативная основа защиты ПДн в Российской Федерации. Назначение модели угроз. Основные задачи, решаемые с применением модели угроз. Угрозы безопасности ПДн в модели угроз. сновные понятия в модели угроз. Общая структура угроз. Структура «Базовой модели угроз безопасности ПД при их обработке в ИСПД. Акустические каналы утечки информации. Классификация технических каналов утечки акустической информации (ТКУАИ). Прямой акустический (воздушный) канал утечки. Акустовибрационный канал утечки. Прямой вибрационный канал. Составной виброакустический канал. Акустоэлектрические каналы утечки информации. Элементы, обладающие микрофонным эффектом. Акустоэлектромагнитные (параметрические) каналы утечки акустической информации. Классификация (ТКУАИ). Классификация угроз безопасности персональных данных.	ЛК, СЗ
		3.2	Классификация угроз ENISA Threat Taxonomy	Введение в ENISA и его роль в кибербезопасности. Основные документы ENISA по классификации угроз. Структура и цель ENISA Threat Taxonomy. Иерархическая структура угроз: 9 основных категорий. Применение классификации: сценарии использования. Детализация категорий угроз. Источники	ЛК, СЗ
		3.3	Классификация уязвимостей	Введение в классификацию уязвимостей. Международные	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				системы классификации и оценки уязвимостей. Национальная классификация по ГОСТ Р 56546-2015. Классификация уязвимостей в системах обработки персональных данных (ФСТЭК). CWE — систематизация недостатков программного обеспечения. Иерархия абстракции и представления в CWE. Основные представления (Views) в CWE. Структура записи в CWE	
Раздел 4	Идентификация, анализ и оценка уязвимостей.	4.1	Типы оценок уязвимостей	Понятие идентификации уязвимостей. Анализ уязвимостей: определение и задачи. Оценка уязвимостей: процесс и этапы. Сравнение оценки и анализа уязвимостей. Типы оценки уязвимостей. Рекомендации по оценке уязвимостей	ЛК, СЗ
		4.2	Основные подходы к выявлению уязвимостей в информационных системах	Введение в процессы выявления уязвимостей. Автоматизированные инструментальные средства поиска уязвимостей. Тестирование и оценка безопасности информационных систем. Анализ программного обеспечения на наличие уязвимостей. Тестирование на проникновение (пентест). Сравнительный анализ оценки уязвимостей и пентеста. Интеграция методов в практике управления безопасностью.	ЛК, СЗ
		4.3	Сравнение основных методологий анализа и оценки уязвимостей	Сравнение основных методологий анализа и оценки уязвимостей.	ЛК, СЗ
		4.4	Приоритизация выявленных уязвимостей	Актуальность приоритизации уязвимостей. Проблемы традиционных подходов. Методологии и подходы (низкий уровень). Стандартные системы (средний уровень). Специализированные системы (высокий уровень). Рекомендации по построению эффективной стратегии	ЛК, СЗ
		4.5	Система оценки критичности уязвимостей CVSS (Common Vulnerability Scoring System)	Общие сведения о системе CVSS. Версии стандарта CVSS: хронология и статус. Группы метрик в CVSS 3.0 и 3.1. Базовые метрики CVSS 3.1. Временные метрики. Контекстные метрики. Основные изменения в руководстве CVSS v3.1. Качественная шкала. Векторная строка. CVSS v4.0 — архитектурное обновление стандарта. Текущее состояние внедрения CVSS v4.0.	ЛК, СЗ
		4.6	Прогнозирования вероятности эксплуатации уязвимости с помощью методологии EPSS (Exploitability,	Общее определение EPSS. Принципы работы EPSS.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			Prevalence, and Severity Score)		
		4.7	Методика оценки критичности уязвимостей CISA SSVC (Stakeholder-Specific Vulnerability Categorization)	Причины разработки методики оценки критичности уязвимостей. Решения по уязвимости в CISA. Основные критерии оценки (точки принятия решений). Дерево решений SSVC: комплексный подход к приоритизации уязвимостей.	ЛК, СЗ

* - 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.	Компьютер/ноутбук, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели 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.	Компьютер/ноутбук, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей.

2. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148383 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

Дополнительная литература:

1. Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)» (утв. ФСТЭК России 17.05.2023)

2. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

3. ГОСТ Р 58142-2018. Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения

в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей. – Введ. 01.11.2018. – М.: Стандартинформ, 2018. – Режим доступа: https://base.garant.ru/72160976/.

4. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. – Gaithersburg: NIST, 2012

5. ENISA Threat Landscape Report 2016 15 Top Cyber-Threats and Trends

6. Common Vulnerability Scoring System v4.0 Specification Document. – FIRST.org, 2023

7. Exploit Prediction Scoring System (EPSS) Model v3. – FIRST.org, 2024. – Режим доступа: https://orca.security/resources/blog/epss-scoring-system-explained/.

8. Stakeholder-Specific Vulnerability Categorization (SSVC) CISA / Carnegie Mellon SEI, 2023. – Режим доступа: https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – ФСТЭК России, 2019

10. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утв. ФСТЭК России 30.06.2025). – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/412283948/.

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 «Источники угроз кибербезопасности и анализ уязвимостей».

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

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Ботвинко Анатолий Юрьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*