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

СТАТИСТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В КИБЕРБЕЗОПАСНОСТИ
(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 «Статистическое моделирование в кибербезопасности» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 7 разделов и 19 тем и направлена на изучение статистических методов прогнозирования киберугроз, обнаружения аномалий в сети, количественное оценивание рисков и принятия обоснованных решений по защите информационных систем в условиях неопределенности и неполноты данных.

Целью освоения дисциплины является развитие у слушателей базовых знаний в области статистического моделирования и расширение навыков применения этих знаний для решения различных проблем кибербезопасности, формирование у студентов необходимой теоретической базы и практических навыков, которые позволят всесторонне и системно понимать современные проблемы прикладной математики и информатики, проблемы обработки и анализа информации, а также умение разрабатывать и анализировать концептуальные и теоретические модели при решении научных и прикладных задач в области кибербезопасности. Главная задача курса - сформировать целостное представление о современных проблемах статистического моделирования, помочь овладеть опытом разработки и анализа концептуальных и теоретических моделей для решения различных вопросов кибербезопасности. В данном курсе рассматриваются наиболее значимые с данной точки зрения разделы статистического моделирования. Изучение данного курса является важной частью профессионального образования будущего магистра, специализирующегося в области фундаментальной информатики и информационных технологий.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Статистическое моделирование в кибербезопасности» 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)
ПК-3	Проведение анализа безопасности компьютерных систем	ПК-3.1 Знает уязвимости компьютерных систем и сетей; ПК-3.2 Знает криптографические методы защиты информации; ПК-3.3 Знает принципы построения систем управления базами данных; ПК-3.4 Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия; ПК-3.5 Умеет разрабатывать предложения по устранению выявленных уязвимостей; ПК-3.6 Умеет составлять и оформлять аналитический отчет по результатам проведенного анализа;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Статистическое моделирование в кибербезопасности» относится к блоку по выбору блока образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Статистическое моделирование в кибербезопасности».

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

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
ПК-3	Проведение анализа безопасности компьютерных систем	Обеспечение безопасности в сетях передачи данных; Методы математического моделирования в кибербезопасности;	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 «Статистическое моделирование в кибербезопасности» 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)**
			3
Контактная работа, ак.ч.	*54*		*54*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	36		36
Самостоятельная работа обучающихся, ак.ч.	*63*		*63*
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	Байесовские модели в кибербезопасности (КБ)	1.1	Байесовские сети в КБ	Понятие байесовской сети (направленный ациклический граф, условные вероятности). Цепное правило для байесовских сетей. Механизмы логического вывода и принятия решений в условиях неопределенности на основе Байеса	ЛК, СЗ
		1.2	Иерархические байесовские модели	Понятие иерархической байесовской модели (Hierarchical Bayesian Model, HBM). Многоуровневая структура: гиперприоры и гиперпараметры. Сравнение с «плоскими» моделями. Методы статистического вывода (Марковские цепи Монте-Карло, вариационный вывод). Практическое применение (A/B тестирование, рейтинговые системы, биостатистика).	ЛК, СЗ
		1.3	Байесовская регрессия	Байесовский подход к регрессионному анализу. Отличие от классического (частотного) метода наименьших квадратов. Априорные и апостериорные распределения параметров. Прогнозирование в байесовской регрессии.	ЛК, СЗ
		1.4	Байесовская модель пространственно - временного ряда	Байесовский подход к моделированию пространственно-временных данных. Пространственные эффекты (соседство, расстояния) и временные лаги. Методы вывода и прогнозирования в байесовских ПВР-моделях.	ЛК, СЗ
Раздел 2	Метод Монте- Карло в КБ	2.1	Оценка рисков кибератак методом Монте-Карло	Имитационное моделирование киберрисков методом Монте-Карло. Генерация случайных сценариев атак. Оценка функции распределения ущерба (VaR, CVaR). Сходимость и точность метода.	ЛК, СЗ
		2.2	Прогнозирование устойчивости сетей к DDoS-атакам с помощью метода Монте-Карло	Имитационное моделирование DDoS-атак методом Монте-Карло. Генерация сценариев распределенных отказов в обслуживании. Оценка показателей QoS (пропускная способность, задержка, процент потерянных пакетов). Построение доверительных интервалов для времени отказа сети (MTTF).	ЛК, СЗ
		2.3	Моделирование социально-инженерных атак с помощью симуляций	Вероятностное и имитационное моделирование социально-инженерных атак. Марковские процессы принятия решений (MDP) и обучение с подкреплением (RL) для анализа поведения злоумышленника. Скрытые марковские модели	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				(HMM) для оценки скрытых состояний жертвы	
		2.4	Оптимизация распределения ресурсов в сфере КБ с помощью метода Монте-Карло	Вероятностная оптимизация распределения ресурсов защиты информационных систем на основе метода Монте-Карло. Моделирование рисков и стохастических сценариев. Многокритериальная задача минимизации ожидаемого ущерба при бюджетных ограничениях.	ЛК, СЗ
Раздел 3	Анализ стандартного отклонения и его применение в КБ	3.1	Суть метода и примеры его применения в КБ	Дескриптивная статистика и анализ стандартного отклонения в задачах мониторинга ИБ. Вычисление выбросов на основе правила «трёх сигм» (3σ). Оценка стабильности работы систем защиты. Квантильный анализ для определения порогов срабатывания IDS/IPS.	ЛК, СЗ
		3.2	Анализ сетевого трафика (Network Traffic Analysis, NTA) с целью обнаружения кибератак	Методы и технологии анализа сетевого трафика для обнаружения компьютерных атак. Deep Packet Inspection (DPI), Flow-анализ, поведенческие детекторы. Применение машинного обучения и сигнатурного анализа для классификации угроз.	ЛК, СЗ
		3.3	Анализ журналов событий с целью выявления некорректного поведения пользователей)	Технологии поведенческого анализа пользователей (UEBA) на основе журналов событий. Сбор, нормализация и корреляция логов (Windows Event Logs, Syslog, журналы приложений). Методы обнаружения аномалий: временные, частотные и паттерн-анализ.	ЛК, СЗ
Раздел 4	Квантильная регрессия и ее применение в кибербезопасности	4.1	Суть метода квантильной регрессии и ее применение в КБ	Метод квантильной регрессии для условных квантилей зависимой переменной. Минимизация взвешенной суммы модулей ошибок. Применение в КБ для построения доверительных интервалов трафика, выявления всплесков активности (burst-атак) и оценки рисков при частичной информации об уязвимостях.	ЛК, СЗ
Раздел 5	Дисперсионный анализ в КБ	5.1	Суть дисперсионного анализа и примеры его применения в КБ	Однофакторный и многофакторный дисперсионный анализ для проверки гипотез о равенстве средних в нескольких группах. F-критерий Фишера. Применение в КБ: выявление значимых факторов, влияющих на количество инцидентов; сравнение уровней защищенности сегментов сети; анализ эффективности мер реагирования.	ЛК, СЗ
		5.2	Обнаружение вторжений в телекоммуникационных системах и сетях с помощью дисперсионного анализа	Применение дисперсионного анализа для выявления аномалий сетевого трафика и обнаружения вторжений. Проверка гипотез об однородности распределений.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 6	Марковские модели в кибербезопасности	6.1	Цепи Маркова и их применение в КБ	Марковские модели кибератак и их использование для анализа защищенности информационных систем. Вычисление метрик безопасности (среднее время до отказа, риск).	ЛК, СЗ
		6.2	Марковские процессы и их применение в КБ	Марковские случайные процессы: основные понятия и классификация (цепи Маркова, марковские процессы принятия решений, полумарковские процессы). Применение в кибербезопасности: моделирование динамики кибератак, оценка временных характеристик защищенности, количественный анализ рисков информационной безопасности.	ЛК, СЗ
Раздел 7	Временные ряды в КБ	7.1	Семейство моделей ARIMA и их применение в КБ	Семейство моделей ARIMA (AutoRegressive Integrated Moving Average): структура, компоненты (p, d, q) и порядок идентификации. Применение в задачах кибербезопасности: прогнозирование временных рядов сетевого трафика, обнаружение аномалий и атак, оценка трендов уязвимостей.	ЛК, СЗ
		7.2	Семейство моделей ETS и их применение в КБ	Семейство моделей ETS (Exponential Smoothing State Space — экспоненциальное сглаживание в пространстве состояний): структура, компоненты (ошибка, тренд, сезонность) и методы идентификации. Применение в задачах кибербезопасности: прогнозирование киберугроз, обнаружение сетевых аномалий, анализ временных рядов атак.	ЛК, СЗ
		7.3	Анализ вредоносной активности с помощью моделей LSTM	Анализ вредоносной активности с использованием моделей LSTM (долгая краткосрочная память). Обработка последовательных данных (сетевой трафик, API-вызовы, системные логи). Применение для обнаружения атак реального времени и классификации вредоносного ПО.	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.	
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 с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, Яндекс Телемост

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Макшанов А.В., Журавлев А.Е., Тындыкарь Л.Н. Большие данные. Big data: учебник для вузов.2021.Изд-во Лань. 186 с.

2. Ватьян А.С., Добренко Н.В., Гусарова Н.Ф. Data science: проблемы и решения. Изд-во Национального Исследовательский Университета ИТМО, 2025. 221 с.

3. Путко, Б.А. Эконометрика : учебник / Б.А. Путко, Н.Ш. Кремер ; ред. Н.Ш. Кремер. - 3-е изд., перераб. и доп. - Москва : Юнити-Дана, 2012. - 329 с. - (Золотой фонд российских учебников). - ISBN 978-5-238-01720-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=118251

4. Бочаров Павел Петрович. Теория вероятностей и математическая статистика [текст] : Учебное пособие / П.П. Бочаров, А.В. Печинкин. - М. : Физматлит, 2005. - 295 с. : ил. - ISBN 5-9221-0633-3 : 153.00. (ET 100)

5. Буравлев Александр Иванович. Эконометрика [Текст/электронный ресурс] : Учебное пособие / А.И. Буравлев. - Электронные текстовые данные. - М. : БИНОМ. Лаборатория знаний, 2019. - 164 с. : ил. - ISBN 978-5-9963-0741-8 : 220.00. Режим доступа: http://lib.rudn.ru/ProtectedView/Book/ViewBook/6768

6. П. А. Панилов. Использование байесовских моделей и методов Монте-Карло для

прогнозирования киберугроз// Вестник Астраханского ГТУ- 2024. №4

Дополнительная литература:

1. Томас Нилд. Математика для Data Science. Управляем данными с помощью линейной алгебры, теории вероятностей и статистики.- Изд-во: Sprint Book/- 2024.- 352 с.

2. Cybersecurity for Smart Grid Systems URL: https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems (Last accessed: 25 June 2018)

3. Lightweight Stream Ciphers for Green IT Engineering / Kuznetsov O. and all. Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 113 – 137.

4. Trapeznikov E.V., Magazev A.A., Kasenov A.A. The Markov model of cyber attacks and its application to the analysis of information security in automated systems. Modeling, Optimization and Information Technology. 2024;12(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1554 DOI: 10.26102/2310-6018/2024.45.2.011 (In Russ.)

5. Prospective Lightweight Block Cipher for Green IT Engineering /Andrushkevych A. and all. Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control. 2019. Vol. 171. P. 95 – 112.

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 «Статистическое моделирование в кибербезопасности».

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

РАЗРАБОТЧИКИ:

Доцент кафедры теории вероятностей и кибербезопасности		Матюшенко Сергей Иванович
Должность, БУП	*Подпись*	*Фамилия И.О.*
Ассистент кафедры теории вероятностей и кибербезопасности		Ермолаева Анна Михайловна
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.*