МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ДЛЯ ПОСТУПАЮЩИХ В МАГИСТРАТУРУ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ «09.04.03 – ПРИКЛАДНАЯ ИНФОРМАТИКА»

магистерская программа

«Искусственный интеллект в кибербезопасности»

РАЗДЕЛ 1. ОСНОВЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

(общепрофессиональный блок, доступный выпускникам любых IT-направлений)

Тема 1.1. Введение в искусственный интеллект

1. Определение искусственного интеллекта (ИИ). История возникновения и развития.
2. Философские аспекты ИИ: слабый, сильный, гиперинтеллект.
3. Основные направления исследований: представление знаний, рассуждения, обучение, восприятие, обработка естественного языка.
4. Связь ИИ с другими дисциплинами: математика, статистика, психология, нейрофизиология.
5. Этические и социальные проблемы ИИ: ответственность, дискриминация, прозрачность, «чёрный ящик».

Тема 1.2. Данные и знания

1. Понятие данных, информации, знаний.
2. Источники данных: структурированные, полуструктурированные, неструктурированные.
3. Качество данных: полнота, непротиворечивость, достоверность.
4. Предобработка данных: очистка, нормализация, стандартизация, работа с пропусками.
5. Разведочный анализ данных (EDA): визуализация, описательные статистики.
6. Формирование обучающей, валидационной и тестовой выборок.

Тема 1.3. Классификация задач машинного обучения

1. Обучение с учителем (supervised learning): классификация, регрессия, прогнозирование.
2. Обучение без учителя (unsupervised learning): кластеризация, снижение размерности, ассоциативные правила.

3. Обучение с подкреплением (reinforcement learning): агент, среда, награда, политика.
4. Активное обучение, трансферное обучение, федеративное обучение (обзорно).
5. Онлайн-обучение и обучение на потоках данных.

Тема 1.4. Классические алгоритмы машинного обучения

1. Линейные модели:
   - Линейная регрессия: метод наименьших квадратов.
   - Логистическая регрессия: сигмоидная функция, граница решения.
   - Регуляризация: L1 (Lasso), L2 (Ridge), ElasticNet.
2. Метрические методы:
   - Метод k-ближайших соседей (kNN).
   - Взвешенные kNN, выбор метрики (Евклид, Манхэттен, косинусная мера).
3. Решающие деревья:
   - Энтропия, прирост информации, индекс Джини.
   - Жадный алгоритм построения, критерии остановки.
   - Проблема переобучения: стрижка (pruning).
4. Ансамблевые методы:
   - Бэггинг (Bagging): случайный лес (Random Forest).
   - Бустинг (Boosting): AdaBoost, градиентный бустинг (XGBoost, LightGBM, CatBoost).
   - Стекинг (Stacking).
5. Метод опорных векторов (SVM):
   - Идея максимизации зазора.
   - Ядровой приём (kernel trick).

Тема 1.5. Кластеризация и снижение размерности

1. Кластеризация:
   - Иерархическая кластеризация (агломеративная, дивизимная).
   - Алгоритм k-средних (k-means), выбор числа кластеров.
   - DBSCAN, OPTICS: кластеризация на основе плотности.
2. Снижение размерности:
   - Метод главных компонент (PCA).
   - t-SNE, UMAP (обзорно).
   - Автоэнкодеры (простейшие нейросетевые).

Тема 1.6. Введение в нейронные сети и глубокое обучение

1. Биологический нейрон и формальный нейрон Маккаллока–Питтса.
2. Однослойный персептрон, ограничения.
3. Многослойный персептрон (MLP): скрытые слои, нелинейности (ReLU, sigmoid, tanh).
4. Алгоритм обратного распространения ошибки.
5. Функции потерь: MSE, кросс-энтропия.
6. Оптимизаторы: SGD, Momentum, Adam.
7. Проблемы обучения глубоких сетей: затухание/взрыв градиента, переобучение.
8. Регуляризация в нейросетях: Dropout, Batch Normalization.

Тема 1.7. Оценка качества моделей

1. Метрики для классификации:
   - Матрица ошибок (confusion matrix).
   - Accuracy, precision, recall, F1-мера.
   - ROC-кривая, AUC-ROC.
   - Логарифмическая функция потерь (log-loss).
2. Метрики для регрессии:
   - MAE, MSE, RMSE, R^2.
3. Метрики для кластеризации:
   - Silhouette score, индекс Дэвиса–Боулдина.
4. Методы валидации:
   - Hold-out, кросс-валидация (k-fold, stratified k-fold).
   - Сравнение моделей: дилемма смещения-дисперсии.

РАЗДЕЛ 2. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(базовые понятия, необходимые для понимания проблематики ИИ в защите)

Тема 2.1. Введение в кибербезопасность

1. Понятия: информационная безопасность, кибербезопасность, защита информации.
2. Основные свойства защищаемой информации: конфиденциальность, целостность, доступность (триада CIA).
3. Дополнительные свойства: аутентичность, неотказуемость, подотчётность.
4. Угрозы, уязвимости, риски, атаки – соотношение понятий.
5. Классификация угроз: природные, техногенные, антропогенные (умышленные/неумышленные).
6. Модель нарушителя: внутренний/внешний, уровень привилегий, цели.

Тема 2.2. Криптографические методы защиты

1. Основные понятия: шифрование, дешифрование, ключ, криптосистема.
2. Симметричные криптосистемы: принцип, примеры (AES, ГОСТ 28147-89, «Магма»).
3. Асимметричные криптосистемы: принцип, открытый/закрытый ключ (RSA, ECC).
4. Хеш-функции: свойства (необратимость, устойчивость к коллизиям), примеры (MD5, SHA-1, SHA-2/3, ГОСТ Р 34.11-2012).
5. Электронная подпись (ЭП, ЭЦП): назначение, схема работы.
6. Инфраструктура открытых ключей (PKI), цифровые сертификаты.

Тема 2.3. Сетевая безопасность

1. Модель OSI и стек TCP/IP: уязвимости уровней.
2. Межсетевые экраны (FW): пакетные фильтры, stateful inspection, NGFW.
3. Системы обнаружения и предотвращения вторжений (IDS/IPS): сигнатурные, поведенческие.
4. Виртуальные частные сети (VPN): IPSec, OpenVPN, WireGuard.

5. Безопасность беспроводных сетей: WEP, WPA, WPA2, WPA3.
6. Протоколы SSL/TLS: рукопожатие, шифрование, сертификаты.

Тема 2.4. Безопасность приложений и баз данных

1. OWASP Top 10: актуальный перечень угроз для веб-приложений.
2. Инъекции: SQL-инъекции, NoSQL-инъекции, LDAP-инъекции – принципы и защита.
3. Межсайтовый скриптинг (XSS): отражаемый, сохранённый, DOM-based.
4. Межсайтовая подделка запроса (CSRF).
5. Небезопасная прямая ссылка на объект (IDOR).
6. Управление сессиями и аутентификацией.
7. Безопасность баз данных: управление доступом, шифрование данных в покое и при передаче, аудит.
8. Принципы безопасного программирования (SDLC, DevSecOps).

Тема 2.5. Вредоносное программное обеспечение

1. Классификация вредоносного ПО: вирусы, черви, трояны, шпионское ПО, программы-вымогатели (ransomware), бэкдоры, руткиты.
2. Методы распространения и маскировки.
3. Сигнатурный и эвристический анализ.
4. Поведенческий анализ и песочницы (sandbox).
5. Современные тенденции: полиморфизм, метаморфизм, APT-атаки.

Тема 2.6. Организационно-правовые аспекты

1. Законодательство РФ в области защиты информации: Конституция РФ, ГК РФ, КоАП, УК РФ.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» (149-ФЗ).
3. Федеральный закон «О персональных данных» (152-ФЗ).
4. Лицензирование и сертификация во ФСТЭК, ФСБ России.
5. Стандарты ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 57580 (для финансовой сферы).
6. Политика информационной безопасности организации.

РАЗДЕЛ 3. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

(интегративный раздел, демонстрирующий способность абитуриента соединять знания из областей ИИ и ИБ)

Тема 3.1. Обнаружение вторжений на основе машинного обучения

1. Сетевые системы обнаружения вторжений (NIDS): сбор трафика, извлечение признаков.
2. Наборы данных: KDD Cup 99, NSL-KDD, CICIDS2017/2019, UNSW-NB15.
3. Применение логистической регрессии, случайного леса, градиентного бустинга.

4. Глубокие нейронные сети для обнаружения аномалий (Autoencoder, LSTM).
5. Проблема несбалансированных классов: oversampling (SMOTE), undersampling, взвешивание классов.

Тема 3.2. Интеллектуальный анализ защищённости (AI-пентинг)

1. Автоматизация сбора информации о целях (OSINT) с помощью NLP.
2. Генерация тестовых сценариев для поиска уязвимостей (фаззинг с обучением).
3. Применение обучения с подкреплением для моделирования действий атакующего.
4. Предсказание наиболее вероятных векторов атак.

Тема 3.3. NLP в кибербезопасности

1. Анализ текстов уязвимостей (CVE, CWE) – автоматическое извлечение сущностей.
2. Обнаружение фишинговых писем: контент-анализ, лингвистические признаки, анализ заголовков.
3. Классификация вредоносных URL и доменов по их лексическим признакам.
4. Анализ кода на наличие уязвимостей с использованием языковых моделей (CodeBERT, GraphCodeBERT).

Тема 3.4. Защита систем искусственного интеллекта

1. Состязательные атаки (adversarial attacks):
   - Методы создания состязательных примеров: Fast Gradient Sign Method (FGSM), Projected Gradient Descent (PGD).
   - Атаки на этапе обучения (отравление данных, poisoning).
   - Атаки на этапе вывода (увод, evasion).
2. Методы защиты:
   - Состязательное обучение (adversarial training).
   - Градиентная маскировка, дистилляция.
   - Обнаружение состязательных примеров.
3. Конфиденциальность данных в ИИ:
   - Дифференциальная приватность (differential privacy).
   - Гомоморфное шифрование.
   - Федеративное обучение (federated learning).

Тема 3.5. Безопасность больших данных и облачных систем

1. Особенности защиты распределенных вычислительных систем (Hadoop, Spark).
2. Управление доступом в озёрах данных (data lakes).
3. Безопасность контейнеров (Docker) и оркестраторов (Kubernetes).
4. IAM (Identity and Access Management) в облаках (AWS IAM, Azure AD).
5. Data Loss Prevention (DLP) с использованием поведенческого анализа.

Тема 3.6. Биометрическая аутентификация и ИИ

1. Распознавание лиц, отпечатков пальцев, голоса.
2. Нейросетевые методы сравнения биометрических образцов.
3. Уязвимости биометрических систем: спуфинг, Deepfake, атаки презентации.
4. Liveness detection: методы борьбы с подделками.
5. Этические и правовые ограничения биометрии.

Тема 3.7. Прогнозирование и предотвращение атак

1. Применение временных рядов в задачах безопасности (анализ логов, сетевого трафика).
2. LSTM и GRU для прогнозирования аномалий.
3. Оценка киберрисков с помощью вероятностных графических моделей.
4. Системы класса UEBA (User and Entity Behavior Analytics).

4.1. Основная литература

Искусственный интеллект и машинное обучение:

1. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / пер. с англ. А. А. Слинкина. – 3-е изд. – М.: ДМК Пресс, 2025. – 1056 с.
2. Рассел С., Норвиг П. Искусственный интеллект. Современный подход / пер. с англ. А. В. Хачко. – 5-е изд. – М.: Вильямс, 2023. – 1408 с.
3. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с англ. А. А. Слинкина. – 3-е изд., испр. – М.: ДМК Пресс, 2024. – 652 с.
4. Нильсон М. Глубокое обучение для безопасных систем / пер. с англ. – М.: Бомбора, 2024. – 416 с.
5. Брюс П., Брюс Э. Практическая статистика для специалистов Data Science / пер. с англ. – СПб.: Питер, 2025. – 416 с.
6. Мюллер А. С., Гвидо С. Введение в машинное обучение с помощью Python. – М.: Вильямс, 2023. – 480 с.
7. Чжан А., Липтон З. К., Ли М., Смола А. Дж. Машинное обучение: разумное и глубокое / пер. с англ. – СПб.: Питер, 2024. – 672 с.
8. Бурков А. Машинное обучение без лишних слов. – СПб.: Питер, 2023. – 320 с.
9. Джеймс Г., Уиттон Д., Хасти Т., Тибширани Р. Введение в статистическое обучение с примерами на Python / пер. с англ. – М.: Диалектика, 2025. – 768 с.
10. Гéрон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow. – 3-е изд. – СПб.: Питер, 2026. – 848 с.
11. Вандер Плас Дж. Python для сложных задач. Наука о данных и машинное обучение. – СПб.: Питер, 2024. – 576 с.
12. Шолле Ф. Глубокое обучение на Python. – 2-е изд. – СПб.: Питер, 2025. – 576 с.
13. Траск Э. Глубокое обучение: самые важные алгоритмы с примерами кода / пер. с англ. – М.: ДМК Пресс, 2023. – 360 с.
14. Кунина О.О. Основы искусственного интеллекта: учебное пособие. – СПб.: Лань, 2025. – 312 с.
15. Соснин П.И. Введение в искусственный интеллект: учебник. – М.: Юрайт, 2026. – 450 с.

Кибербезопасность:

16. Столлингс В., Браун Л. Безопасность беспроводных сетей и мобильных устройств / пер. с англ. – М.: Вильямс, 2025. – 560 с.
17. Столлингс В. Криптография и защита сетей. Принципы и практика. – 8-е изд. – М.: Вильямс, 2024. – 928 с.
18. Васильев Н.П. Искусственный интеллект в задачах кибербезопасности: учебное пособие. – СПб.: Лань, 2024. – 312 с.
19. Чио К., Фримэн Д. Машинное обучение и безопасность / пер. с англ. А. В. Слинкина. – СПб.: Питер, 2023. – 480 с.
20. Роуз Д. Технологии защиты данных в системах искусственного интеллекта. – М.: ДМК Пресс, 2025. – 288 с.
21. Батура Т.В., Мурзин Ф.А. Методы и системы искусственного интеллекта: учебник. – М.: Юрайт, 2024. – 484 с.
22. Шакирьянов Э.Д. Компьютерные сети и кибербезопасность: учебник для вузов. – СПб.: Лань, 2025. – 380 с.
23. Котенко И.В., Саенко И.Б. Интеллектуальные системы кибербезопасности: модели и методы. – М.: Наука, 2024. – 440 с.
24. Малюк А.А., Погожин Н.С. Теория информационной безопасности. Методологические основы. – М.: Горячая линия – Телеком, 2023. – 192 с.
25. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2024. – 600 с.
26. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 7-е изд. – СПб.: Питер, 2025. – 1008 с.
27. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 6-е изд. – СПб.: Питер, 2024. – 1024 с.
28. Мессие Ж. Безопасность контейнеров. Фундаментальный подход к защите контейнеризованных приложений / пер. с англ. – М.: ДМК Пресс, 2024. – 468 с.
29. Липский В.В. Информационная безопасность государства и личности. – М.: Инфра-М, 2025. – 320 с.
30. Варлатая С.К., Шаханова М.В. Кибербезопасность: основные понятия и определения. – Владивосток: ДВФУ, 2023. – 214 с.

Базы данных и инструментарий:

31. Грофф Дж., Вайнберг П., Оппель Э. SQL. Полное руководство. – 4-е изд. – М.: Вильямс, 2025. – 1088 с.
32. Мартишин С.А., Симонов В.Л., Храпченко М.В. Проектирование и реализация баз данных в СУБД MySQL. – М.: Форум, 2024. – 160 с.
33. Лубенская Е.В. Большие данные: технологии обработки и хранения. – Ростов н/Д: Феникс, 2025. – 256 с.
34. Дрёмов С.В., Марков А.С. Технологии Big Data в защите информации. – М.: Радиотехника, 2024. – 296 с.
35. Гроссман Л. SQL для анализа данных. – СПб.: Питер, 2025. – 448 с.

4.2. Дополнительная литература и специализированные издания

36. Аверкин А.Н., Ярушев С.А. Мягкие вычисления и нечёткая логика в системах защиты информации. – М.: Физматлит, 2023. – 288 с.
37. Алпайдин Э. Введение в машинное обучение с подкреплением / пер. с англ. – М.: ДМК Пресс, 2024. – 384 с.
38. Жерон О. Применение глубокого обучения для анализа безопасности сетей / пер. с англ. – СПб.: Питер, 2025. – 512 с.
39. Золкин А.Л., Никитин А.Л. Базы знаний и экспертные системы в интеллектуальных системах безопасности: учебное пособие. – М.: Русайнс, 2024. – 208 с.
40. Льюис Н.Д. Глубокое обучение для NLP и компьютерного зрения в задачах информационной безопасности / пер. с англ. – М.: Вильямс, 2024. – 528 с.
41. Корнеев В.В. Прикладные программные архитектуры. Интеллектуальные агенты и мультиагентные системы. – 3-е изд. – М.: Юрайт, 2025. – 313 с.
42. Турнецкая Е.Л. Безопасность программного обеспечения и интеллектуальных систем: учебник. – СПб.: Лань, 2024. – 288 с.
43. Борзунов С.В., Кургалин С.Д. Языки программирования. Python: решение сложных задач. – СПб.: Лань, 2023. – 192 с.
44. Макшанов А.В., Журавлев А.Е. Технологии интеллектуального анализа данных. – 2-е изд. – СПб.: Лань, 2022. – 212 с.
45. Хомоненко А.Д. и др. Модели и методы исследования информационных систем. – СПб.: Лань, 2022. – 204 с.
46. Ткаченко С.Н., Мищук Б.Р. Методы и средства проектирования информационных систем и технологий. – М.: КноРус, 2022. – 222 с.
47. Цехановский В.В., Чертовской В.Д. Управление данными. – СПб.: Лань, 2022. – 432 с.
48. Абдуллаева О.С., Исомиддинов А.И., Абдуллаева С.Х. Информационные технологии. – М.: Русайнс, 2024. – 189 с.
49. Ратушняк Г.Я., Золкин А.Л., Никитин А.Л. Базы данных: учебное пособие. – М.: Русайнс, 2024. – 127 с.
50. Голицына О.Л., Максимов Н.В., Попов И.И. Информационные системы и технологии: учебное пособие. – М.: Форум, 2023. – 400 с.
51. Тюрин И.В. Вычислительная техника и информационные технологии. – 2-е изд. – СПб.: Лань, 2023. – 336 с.
52. Черников Б.В. Информационные технологии управления. – 2-е изд. – М.: Форум, 2023. – 368 с.

Председатель предметной комиссии _____ / С.В. Аникуев /