МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ
В.Ф. УТКИНА»

Кафедра «Вычислительная и прикладная математика»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Защита информации в системах ИИ»

Направление подготовки – 09.03.04 Программная инженерия

ОПОП «Программная инженерия систем искусственного интеллекта»

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная (4 года)

Рязань

1. СПИСОК ТЕОРЕТИЧЕСКИХ ВОПРОСОВ К ЗАЧЁТУ

1. Понятие информации, виды и формы представления информации.
2. История защиты информации и основные этапы её развития.
3. Моделирование угроз и нарушителей в системах ИИ.
4. Риски информационной безопасности и требования к алгоритмам шифрования.
5. Правило Огюста Керкхоффа и его значение для проектирования криптосистем.
6. Симметричные алгоритмы шифрования: общая характеристика.
7. Поточное шифрование: принципы и примеры алгоритмов.
8. Блочные алгоритмы шифрования: принципы и примеры.
9. Шифры перестановки и шифры замены.
10. Моноалфавитные и полиалфавитные шифры.
11. Индекс соответствия и его применение в криптоанализе.
12. Шифровальная машина «Энигма»: принцип работы и криптоанализ.
13. Шифрование с открытым ключом: основные идеи.
14. Алгоритм RSA: математические основы и применение.
15. Генераторы случайных чисел и алгоритм Фон Неймана.
16. Алгоритм на числах Фибоначчи и линейный конгруэнтный генератор.
17. Квадратичный конгруэнтный генератор и нормальное распределение.
18. Алгоритм DES: этапы шифрования и функция Фейстеля.
19. Взлом DES и усовершенствования алгоритма.
20. Открытый конкурс NIST и алгоритм AES.
21. История и особенности асимметричного шифрования.
22. Методы и алгоритмы сжатия данных: общая характеристика.
23. Алгоритм сжатия Хаффмана.
24. Алгоритм сжатия LZW.
25. Математическое сжатие данных.
26. Криптоатаки и методы криптоанализа.
27. Стеганография: назначение, методы и отличия от криптографии.
28. Правовые основы защиты информации.
29. Классификация угроз безопасности для систем ИИ.
30. Атаки на обучающие данные: Data Poisoning.
31. Атаки на вывод модели: Adversarial Attacks.
32. Кража конфиденциальной информации из модели: Model Inversion и Membership Inference.
33. Манипуляция поведением генеративных моделей: prompt injection и jailbreaking.
34. Дифференциальная приватность для защиты данных обучения.
35. Adversarial Training как механизм устойчивости к состязательным атакам.
36. Контроль доступа к API и весам моделей ИИ.
37. Безопасность больших языковых моделей (LLM).
38. Анализ уязвимостей в MLOps-конвейере: Model Replacement Attack.
39. Методы повышения устойчивости, надёжности и безопасности алгоритмов машинного обучения.

40. Особенности безопасности AutoML: риски, методы защиты и подготовка данных.

2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

№	Тема лабораторной работы	Кол-во часов
1	Реализация алгоритма шифрования с открытым ключом (RSA)	4
2	Реализация алгоритма симметричного шифрования (DES)	2
3	Реализация алгоритма симметричного шифрования (AES)	2
4	Исследование устойчивости модели классификации изображений к состязательным атакам (Adversarial Attacks)	4
5	Анализ рисков конфиденциальности в моделях машинного обучения с помощью Membership Inference Attack	4
6	Анализ уязвимостей в MLOps-конвейере: атака через подмену модели (Model Replacement Attack)	4
7	Исследование уязвимости генеративной языковой модели к атакам типа «Инъекция промптов» (Prompt Injection)	4
Итого		**24**

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа как вид учебной работы может использоваться на практических и лабораторных работах, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к практическим и лабораторным работам, при подготовке к зачёту.

Самостоятельная работа включает в себя следующие этапы:

- изучение теоретического материала (работа над конспектом лекции);
- самостоятельное изучение дополнительных информационных ресурсов (доработка конспекта лекции);
- выполнение заданий текущего контроля успеваемости (подготовка к практическим и лабораторным работам);
- итоговая аттестация по дисциплине (подготовка к зачёту).

При подготовке к лабораторным работам необходимо:

1. Изучить конспект лекций и методические указания к данной работе.
2. Ознакомиться с рекомендуемой основной и дополнительной литературой.
3. Выполнить индивидуальное задание.
4. Оформить отчёт в соответствии с требованиями кафедры.
5. Защитить работу, ответив на вопросы преподавателя.

Важным этапом является защита лабораторной работы. В процессе защиты студент отвечает на вопросы преподавателя, касающиеся теоретического материала, относящегося к данной работе, и проекта, реализующего её задание, комментирует полученные результаты. При подготовке к защите рекомендуется ознакомиться со списком вопросов по изучаемой теме и попытаться самостоятельно на них ответить, используя конспект лекций и рекомендуемую литературу.

4. РЕКОМЕНДАЦИИ ПО ПЛАНИРОВАНИЮ И ОРГАНИЗАЦИИ ВРЕМЕНИ, НЕОБХОДИМОГО ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ. ОПИСАНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ СТУДЕНТА («СЦЕНАРИЙ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ»)

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины.

Для освоения лекционного материала следует: изучить конспект лекции в тот же день, после лекции: 10–15 минут, повторно прочитать конспект лекции за день перед следующей лекцией: 10–15 минут. Также следует изучить теоретический лекционный материал по рекомендуемому учебнику/учебному пособию: 1 час в неделю.

Следует максимально использовать лекционное время для изучения дисциплины, понимания лекционного материала и написания конспекта лекций. В процессе лекционного занятия студент должен уметь выделять важные моменты и основные положения. При написании конспекта лекций следует придерживаться следующих правил и рекомендаций:

1. При ведении конспекта рекомендуется структурировать материал по разделам, главам, темам. Вести нумерацию формул. Выделять по каждой теме постановку задачи, основные положения, выводы. Кратко записывать те пояснения лектора, которые показались особенно важными. Это позволит при подготовке к сдаче зачёта не запутаться в структуре лекционного материала.
2. Лекционный материал следует записывать в конспект лишь после того, как излагаемый лектором тезис будет вами дослушан до конца и понят.
3. При конспектировании следует отмечать непонятные на данном этапе положения, доказательства и пр.
4. Рекомендуется по каждой теме выразить своё мнение, комментарий, вывод.

Доработка конспекта лекции с применением учебника, методической литературы, дополнительной литературы, интернет-ресурсов: этот вид самостоятельной работы студентов особенно важен в том случае, когда одну и ту же задачу можно решать различными способами, а на лекции изложен только один из них. Кроме того, рабочая программа предполагает рассмотрение некоторых относительно несложных тем только во время самостоятельных занятий, без чтения лектором.

Подготовка к практическим работам состоит в теоретической подготовке (изучение конспекта лекций, методических указаний к данной практической работе и дополнительной литературы) и выполнении индивидуального задания. Выполнение каждой из запланированных работ заканчивается предоставлением отчёта. Требования к форме и содержанию отчёта приведены в методических указаниях к практическим работам или определяются преподавателем на первом занятии. Допускаясь к практической работе, каждый студент должен представить преподавателю «заготовку» отчёта, содержащую: оформленный титульный лист, цель работы, задание, проект решения, полученные результаты, выводы.

Подготовка к сдаче зачёта.

Зачёт – форма промежуточной проверки знаний, умений, навыков, степени освоения дисциплины. Главная задача зачёта состоит в том, чтобы у студента по окончании изучения данной дисциплины сформировались определённое представление об общем содержании дисциплины, определённые теоретические знания и практические навыки, определённый кругозор. Готовясь к зачёту, студент приводит в систему знания, полученные на лекциях, на практических занятиях, разбирается в том, что осталось непонятным, и тогда изучаемая им дисциплина может быть воспринята в полном объёме с присущей ей строгостью и логичностью, её практической направленностью.

Зачёт даёт возможность преподавателю определить теоретические знания студента и его практические навыки при решении определённых прикладных задач. Оцениваются: понимание и степень усвоения теоретического материала; степень знакомства с основной и дополнительной литературой, а также с современными публикациями; умение применить теорию к практике, решать определённые практические задачи данной предметной области, правильно проводить расчёты и т.

д.; знакомство с историей данной науки; логика, структура и стиль ответа, умение защищать выдвигаемые положения.

Планируйте подготовку к зачёту, учитывая сразу несколько факторов: неоднородность в сложности учебного материала и степени его проработки в ходе обучения, свои индивидуальные способности. Рекомендуется делать перерывы в занятиях через каждые 50–60 минут на 10 минут. После 3–4 часов занятий следует сделать часовой перерыв. Чрезмерное утомление приведёт к снижению тонуса интеллектуальной деятельности. Целесообразно разделять весь рабочий день на три рабочих периода – с утра до обеда, с обеда до ужина и с ужина до сна. Каждый рабочий период дня должен заканчиваться отдыхом не менее 1 часа. Работая в сессионном режиме, студент имеет возможность увеличить время занятий с 10 (как требовалось в семестре) до 12 часов в сутки.

Подготовку к зачёту следует начинать с общего планирования своей деятельности. С определения объёма материала, подлежащего проработке, необходимо внимательно сверить конспекты с программой дисциплины, чтобы убедиться, все ли разделы отражены в лекциях, отсутствующие темы изучить по учебнику. Второй этап предусматривает системное изучение материала по данному предмету с обязательной записью всех выкладок, выводов, формул. На третьем этапе – этапе закрепления – полезно чередовать углублённое повторение особенно сложных вопросов с беглым повторением всего материала.

5. РЕКОМЕНДАЦИИ ПО РАБОТЕ С ЛИТЕРАТУРОЙ

Основная литература, литература для дополнительного чтения и методические указания к практическим (лабораторным) работам указаны в рабочей программе данной дисциплины и доступны посредством ЭБС.

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта изучаются и книги по данному предмету. Литературу по дисциплине рекомендуется читать как в бумажном, так и в электронном виде (если отсутствует бумажный аналог). Полезно использовать несколько учебников и пособий по дисциплине. Рекомендуется после изучения очередного параграфа ответить на несколько вопросов по данной теме. Кроме того, полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): «о чём этот параграф?», «какие новые понятия введены, каков их смысл?», «зачем мне это нужно по специальности?».

Рекомендуется самостоятельно изучать материал, который ещё не прочитан на лекции и не применялся на практическом занятии, тогда занятия будут гораздо понятнее. В течение недели рекомендуется выбрать время (1 час) для работы с литературой.

6. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

6.1. Основная литература

1. Башлы П. Н., Бабаш А. В., Баранова Е. К. Информационная безопасность и защита информации: учебное пособие. – Москва: Евразийский открытый институт, 2012. – 311 с. – ISBN 978-5-374-00301-7. – URL: http://www.iprbookshop.ru/10677.html
2. Евдокимова Л. М., Корябкин В. В., Пылькин А. Н., Швечкова О. Г. Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS: учеб. пособие. – М.: КУРС, 2017. – 294 с.; прил. – ISBN 978-5-906923-24-0, 978-5-16-012741-5.
3. Швечкова О. Г., Пылькин А. Н., Марчев Д. В. Базовые криптографические алгоритмы защиты информации: учеб. пособие. – Рязань: КУРС, 2023. – URL: https://elib.rsreu.ru/ebs/download/3643

6.2. Дополнительная литература

1. Омарова С. А., Искакова К. А., Тойганбаева Н. А. Информационная безопасность и защита информации: учебно-методический комплекс. – Алматы: Нур-Принт, 2012. – 98 с. – ISBN 9965-756-05-8. – URL: http://www.iprbookshop.ru/67055.html
2. Нерсесянц А. А. Защита информации: учебное пособие. – Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. – 61 с. – ISSN 2227-8397. – URL: http://www.iprbookshop.ru/61295.html

6.3. Методические разработки

1. Малинин Ю. И. Информационная безопасность и защита информации: Методические указания. – Рязань: РИЦ РГРТУ, 2009. – URL: https://elib.rsreu.ru/ebs/download/851
2. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Техническая защита информации: лабораторный практикум. – Санкт-Петербург: Университет ИТМО, 2013. – 113 с. – ISSN 2227-8397. – URL: http://www.iprbookshop.ru/68715.html

6.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронная библиотека РГРТУ: https://elib.rsreu.ru/ebs/

6.5. Перечень программного обеспечения и информационных справочных систем

Лицензионное и свободно распространяемое программное обеспечение:

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Python	Свободное ПО
PyCharm Community	Свободное ПО
Jupyter Notebook	Свободное ПО
Adversarial Robustness Toolbox (ART)	Свободное ПО
Библиотеки Python: NumPy, Pandas, Scikit-learn, TensorFlow/PyTorch	Свободное ПО
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО

Информационные справочные системы:

1. Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)
2. Система КонсультантПлюс: http://www.consultant.ru
3. Информационно-правовой портал ГАРАНТ.РУ: http://www.garant.ru