Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
_____ /С.М.Дудаков/
«01» февраля 2024 года

Рабочая программа дисциплины (с аннотацией)

БЕЗОПАСНОСТЬ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Направление подготовки
02.03.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА
И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Направленность (профиль)
Программная инженерия в искусственном интеллекте

Для студентов 4-го курса

Очная форма

Составитель: М.Ю. Кудряшов

Тверь, 2024

I. Аннотация

1. Цель и задачи дисциплины

Цель освоения дисциплины:

— сформировать системное представление об информационной безопасности систем искусственного интеллекта.

Задачами освоения дисциплины являются:

— усвоение системы знаний о базовых основах безопасности систем искусственного интеллекта;

— формирование умений реализовывать прикладные знания в области информационной безопасности в профессиональной деятельности;

— совершенствование методических навыков использования средств безопасности систем искусственного интеллекта в профессиональной деятельности.

2. Место дисциплины в структуре ООП

Данная дисциплина относится к разделу «Гуманитарный» обязательной части Блока 1.

Для успешного освоения дисциплины «Безопасность систем искусственного интеллекта» от обучающегося требуются знания и навыки, полученные в результате изучения курсов по алгебре и геометрии, математическому анализу, дискретной математике, языкам программирования и методам трансляции, компьютерным сетям, операционным системам, архитектуре ЭВМ. Данная дисциплина необходима для изучения дисциплины «Проектирование, разработка и эксплуатация информационных систем».

3. Объем дисциплины: 3 зачетных единицы, 108 академических часов, **в том числе:**

контактная аудиторная работа: лекции 20 часов**,** практические занятия 10 часов*;*

контактная внеаудиторная работа: контроль самостоятельной работы _____, в том числе курсовая работа _____;

самостоятельная работа: 78 часов, в том числе контроль 0 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 Определяет свою роль в социальном взаимодействии и командной работе, исходя из стратегии сотрудничества для достижения поставленной цели УК-3.2 При реализации своей роли в социальном взаимодействии и командной

	работе учитывает особенности поведения и интересы других участников УК-3.3 Анализирует возможные последствия личных действий в социальном взаимодействии и командной работе, и строит продуктивное взаимодействие с учетом этого УК-3.4 Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает идеи других членов команды для достижения поставленной цели УК-3.5 Соблюдает нормы и установленные правила командной работы; несет личную ответственность за результат
УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1 Отмечает и анализирует особенности межкультурного взаимодействия (преимущества и возможные проблемные ситуации), обусловленные различием этических, религиозных и ценностных систем УК-5.2 Предлагает способы преодоления коммуникативных барьеров при межкультурном взаимодействии УК-5.3 Определяет условия интеграции участников межкультурного взаимодействия для достижения поставленной цели с учетом исторического наследия и социокультурных традиций различных социальных групп, этносов и конфессий
ПК-10. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности	ПК-10.1. Выбирает современные технологии и системы искусственного интеллекта для решения задач в профессиональной деятельности ПК-10.2. Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учетом требований информационной безопасности

5. Форма промежуточной аттестации и семестр прохождения - зачет, 8 семестр.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)					Самостоятельная работа, в том числе Контроль (час.)
		Лекции		Практические занятия		Контроль самостоятельной работы (в том числе курсовая работа)	
		всего	в т.ч. практическая подготовка	всего	в т.ч. практическая подготовка		
Основные положения	5	1		0			4
Формальные модели шифров	5	1		0			4
Оценка стойкости блочных шифров	8	2		0			6
Шифр Rijndael (AES)	9	2		1			6
Распределение симметричных ключей	9	2		1			6
Криптографические хеш-функции	9	2		1			6
Схемы открытого шифрования и их стойкость	9	2		1			6
Двухключевые криптосистемы	9	2		1			6
Схемы цифровой подписи и их стойкость	9	2		1			6
Безопасность сети	8	1		1			6
Введение в тему атак на модели машинного обучения	8	1		1			6
Схемы атак	10	1		1			8
Атаки на системы искусственного интеллекта	10	1		1			8
ИТОГО	108	20		10		-	78

III. Образовательные технологии

Учебная программа – наименование разделов и тем *(в строгом соответствии с разделом II РПД)*	Вид занятия	Образовательные технологии
Основные положения	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Формальные модели шифров	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Оценка стойкости блочных шифров	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Шифр Rijndael (AES)	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Распределение симметричных ключей	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Криптографические хеш-функции	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Схемы открытого шифрования и их стойкость	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Двухключевые криптосистемы	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Схемы цифровой подписи и их стойкость	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Безопасность сети	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Введение в тему атак на модели машинного обучения	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач
Схемы атак	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач

Атаки на системы искусственного интеллекта	Лекции, практические занятия	1. Изложение теоретического материала 2. Решение задач

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Для проведения текущей и промежуточной аттестации:

УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

УК-3.1 Определяет свою роль в социальном взаимодействии и командной работе, исходя из стратегии сотрудничества для достижения поставленной цели

Примеры заданий:

1. *Выявление информационных рисков и угроз компьютерным системам (на примере средней школы).*
2. *Разработка мероприятий по управлению рисками и оценке рисков (по лекционным материалам).*

Критерии оценивания:

Сформулировано достаточное количество информационных рисков и угроз – 1 балл.

Правильно использованы ключевые понятия из области компьютерной безопасности и информационных рисков – 1 балл.

Мероприятия, минимизирующие последствия информационных рисков, изложены ясно и логично – 1 балл.

Мероприятия, уменьшающие степень компьютерной безопасности, изложены ясно и логично – 1 балл.

Общая оценка:

2 балла – удовлетворительно.

3 – балла – хорошо.

4 балла – отлично.

3. *Написание рефератов по проблемам обеспечения безопасности систем искусственного интеллекта*
4. *Написание рефератов по методам обеспечения безопасности систем искусственного интеллекта*

Критерии оценивания:

Оригинальность текста составляет свыше 75% - 3 балла

Оригинальность текста составляет 50-74 % - 2 балла

Оригинальность текста составляет 25-49 % - 1 балл

Оригинальность текста составляет менее 25% - 0 баллов

привлечены ли наиболее известные работы по теме исследования (в т.ч. публикации последних лет) – 2 балла

реферат опирается на учебную литературу и/ или устаревшие издания – 1 балл

Отражение в плане ключевых аспектов темы – 2 балла;

Фрагментарное отражение ключевых аспектов темы – 1 балл;

Полное соответствие содержания теме и плану реферата – 2 балла;

Частичное соответствие содержания теме и плану реферата – 1 балла;

сопоставление различных точек зрения по одному вопросу (проблеме) – 1 балла;

Все представленные выводы обоснованы – 2 балла;

Аргументирована часть выводов – 1 балл.

верно оформлены ссылки на используемую литературу – 1 балл

соблюдены правила орфографической, пунктуационной, стилистической культуры – 1 балл;

соблюдены требования к объёму реферата – 1 балл.

УК-3.2 При реализации своей роли в социальном взаимодействии и командной работе учитывает особенности поведения и интересы других участников

УК-3.3 Анализирует возможные последствия личных действий в социальном взаимодействии и командной работе, и строит продуктивное взаимодействие с учетом этого

УК-3.4 Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает идеи других членов команды для достижения поставленной цели

1. *Решение задач по математическим основам криптографических методов защиты информации Решение задач на представления чисел в различных системах счисления и кодировках*
2. *Решение задач по математическим основам обеспечения целостности информации*

Критерии оценивания:

Дан правильный развернутый ответ – 2 балла;

Ответ содержит неточности – 1 балл.

Решение не дано – 0 баллов

УК-5 Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах

УК-5.1 Отмечает и анализирует особенности межкультурного взаимодействия (преимущества и возможные проблемные ситуации), обусловленные различием этических, религиозных и ценностных систем

УК-5.2 Предлагает способы преодоления коммуникативных барьеров при межкультурном взаимодействии

УК-5.3 Определяет условия интеграции участников межкультурного взаимодействия для достижения поставленной цели с учетом исторического

наследия и социокультурных традиций различных социальных групп, этносов и конфессий

1. *Решение задач по методам и средствам обеспечения информационной безопасности компьютерных систем Критерии оценивания:*
   Дан правильный развернутый ответ – 2 балла;
   Ответ содержит неточности – 1 балл.
   Решение не дано – 0 баллов

ПК-10. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности

ПК-10.1. Выбирает современные технологии и системы искусственного интеллекта для решения задач в профессиональной деятельности

ПК-10.2. Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учетом требований информационной безопасности

1. *Разработка порождающей модели МО для генерации изображения лица целевой персоны, позволяющий нарушить работу биометрического классификатора пользователей по лицу. Биометрический классификатор будет предоставлен.*
2. *Разработка порождающей модели МО для генерации голоса целевого диктора, позволяющий нарушить работу биометрического классификатора дикторов по голосу. Биометрический классификатор будет предоставлен.*
3. *Реализация пула состязательных атак, позволяющих нарушить работу биометрического классификатора пользователей по лицу. Биометрический классификатор будет предоставлен.*
4. *Реализация бинарного классификатора синтетических данных, позволяющий идентифицировать такого сорта данные и тем самым защитить модель биометрической классификации лиц. Защита должна эффективно работать от атак, разработанных командой в рамках задания 1. Биометрический классификатор будет предоставлен.*
5. *Реализация механизма состязательного обучения, позволяющего защитить модель биометрической классификации лиц. Защита должна эффективно работать от атак, разработанных командой в рамках задания 3. Биометрический классификатор будет предоставлен.*

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

1. Суворова Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. - 2-е изд. - Электрон. дан. - Москва: Юрайт, 2024. - 277 с. - (Высшее образование). - URL: https://urait.ru/bcode/544029
2. Зенков А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. - 2-е изд. - Электрон. дан. - Москва: Юрайт, 2024. - 107 с. - (Высшее образование). - URL: https://urait.ru/bcode/544290
3. Платонов А. В. Машинное обучение: учебное пособие для вузов / А. В. Платонов. - Электрон. дан. - Москва: Юрайт, 2024. - 85 с. - (Высшее образование). - URL: https://urait.ru/bcode/544780
4. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009
5. Машинное обучение: учебник/Е. Ю. Бутырский [и др.]. - Москва: Директ-Медиа, 2023. - 368 с.: ил., табл., схем., граф. - Библиогр. в кн. - Режим доступа: https://biblioclub.ru/index.php?page=book&id=701807
6. Киренберг А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. - Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. - 138 с. – Режим доступа: https://www.iprbookshop.ru/128393.html

б) Дополнительная литература

1. Гришина Н. В. Основы моделирования процессов и систем защиты информации: учебное пособие / Н. В. Гришина; Российский государственный гуманитарный университет РГГУ. - 1. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 107 с. – Режим доступа: https://znanium.com/catalog/document?id=413938
2. Плас Дж. В. Python для сложных задач: наука о данных и машинное обучение: практическое пособие / Дж. В. Плас - Санкт-Петербург: Питер, 2021. - 576 с. - (Бестселлеры O'Reilly). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=378619
3. Ищейнов В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В. Я. Ищейнов. - Москва, Берлин: Директ-Медиа, 2020. - 271 с.: схем., табл. - Библиогр. в кн. - Режим доступа: https://biblioclub.ru/index.php?page=book&id=571485
4. Маккинли У. Python и анализ данных / У Маккинли; перевод А. Слинкина. - Python и анализ данных. - Электрон. дан. (1 файл). - Саратов: Профобразование, 2019. - 482 с. – Режим доступа: http://www.iprbookshop.ru/88752.html
5. Katy Warr, « Strengthening Deep Neural Networks», O'Reilly Media, 2019.
6. «Adversarial Robustness Toolbox», https://github.com/ Trusted-AI/adversarial-robustness-toolbox
7. Foolbox», https://github.com/bethgelab/foolbox
7. «Cleverhans», https://github.com/cleverhans-lab/cleverhans

8. Шакла, Нишант. Машинное обучение & TensorFlow: [пер. с англ.]. / Нишант Шакла при участии Кена Фрикласа. - СПб. [и др.]: Питер, 2019. - 331, [1] с.; 24 см - (Библиотека программиста).
9. Шолле,Франсуа Глубокое обучение на Python / Франсуа Шолле; [пер. с англ. А. Киселева]. - СПб. [и др.]: Питер, 2020. - 397, [1] с.; 24 см - (Библиотека программиста).

2) Программное обеспечение

Компьютерный класс факультета прикладной математики и кибернетики № 4б (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	
Adobe Acrobat Reader DC - Russian	бесплатно
Apache Tomcat 8.0.27	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
GlassFish Server Open Source Edition 4.1.1	бесплатно
Google Chrome	бесплатно
Java SE Development Kit 8 Update 45 (64-bit)	бесплатно
JetBrains PyCharm Community Edition 4.5.3	бесплатно
JetBrains PyCharm Edu 3.0	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
NetBeans IDE 8.0.2	бесплатно
NetBeans IDE 8.2	бесплатно
Notepad++	бесплатно
Oracle VM VirtualBox 5.0.2	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»
Python 3.1 pygame-1.9.1	бесплатно
Python 3.4 numpy-1.9.2	бесплатно
Python 3.4.3	бесплатно
Python 3.5.1 (Anaconda3 2.5.0 64-bit)	бесплатно
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
R Studio	бесплатно

Anaconda3 2019.07 (Python 3.7.3 64-bit)	бесплатно

Компьютерный класс факультета прикладной математики и кибернетики № 4в (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	
AutoNom Standard	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Deductor Academic	бесплатно
HyperChem	Акт предоставления прав № Tr008313 от 20.02.2016
ISIS Draw 2.4 Standalone	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
KTC Net 3.01	бесплатно
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Oracle VM VirtualBox 5.0.14	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»
Python 3.4.3	бесплатно
Python 3.6.0 (Anaconda3 4.3.0 64-bit)	бесплатно
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

ЭБС **«ZNANIUM.COM»** www.znanium.com;

ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/;

ЭБС **«Лань»** http://e.lanbook.com.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

Интернет-университет http://www.intuit.ru

Электронно-библиотечная система ТвГУ. URL: http://library.tversu.ru
Система ведения учебного процесса по дисциплине через Интернет. URL: http://elearning.tstu.tver.ru
Единое окно доступа к образовательным ресурсам. URL: http://window.edu.ru
Общесистемное программное обеспечение Microsoft Windows 7/8.10, web-браузер (любой доступный).
Программный продукт Microsoft Office 2007/2010/2013.

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации студентам по организации самостоятельной работы.

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке университета, встретиться с преподавателем, ведущим дисциплину, получить в библиотеке рекомендованные учебники и учебно-методические пособия, осуществить запись на соответствующий курс в среде электронного обучения университета.

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

На лекциях важно сосредоточить внимание на ее содержании. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине. Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы. Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

Методические указания для обучающихся по подготовке к семинарским занятиям

Для того чтобы семинарские занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным

разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на семинарских занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач.

При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

При подготовке к семинарским занятиям следует использовать основную литературу из представленного списка, а также руководствоваться приведенными указаниями и рекомендациями. Для наиболее глубокого освоения дисциплины рекомендуется изучать литературу, обозначенную как «дополнительная» в представленном списке.

Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации: изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т. д.; при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы. После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Методические указания для самостоятельной работы обучающихся

Прочное усвоение и долговременное закрепление учебного материала невозможно без продуманной самостоятельной работы. Такая работа требует от студента значительных усилий, творчества и высокой организованности. В ходе самостоятельной работы студенты выполняют следующие задачи: дорабатывают лекции, изучают рекомендованную литературу, готовятся к практическим занятиям, к коллоквиуму, контрольным работам по отдельным темам дисциплины. При этом эффективность учебной деятельности студента во многом зависит от того, как он распорядился выделенным для самостоятельной работы бюджетом времени.

Результатом самостоятельной работы является прочное усвоение материалов по предмету, согласно программы дисциплины. В итоге этой работы формируются профессиональные умения и компетенции, развивается творческий подход к решению возникших в ходе учебной деятельности проблемных задач, появляется самостоятельности мышления.

Решение задач

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи).

Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты.

Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Задача — это цель, заданная в определенных условиях, решение задачи — процесс достижения поставленной цели, поиск необходимых для этого средств.

Алгоритм решения задач:

1. Внимательно прочитайте условие задания и уясните основной вопрос, представьте процессы и явления, описанные в условии.

2. Повторно прочтите условие для того, чтобы чётко представить основной вопрос, проблему, цель решения, заданные величины, опираясь на которые можно вести поиски решения.

3. Произведите краткую запись условия задания.

4. Если необходимо составьте таблицу, схему, рисунок или чертёж.

5. Определите метод решения задания, составьте план решения.

6. Запишите основные понятия, формулы, описывающие процессы, предложенные заданной системой.

7. Найдите решение в общем виде, выразив искомые величины через заданные.

9. Проверьте правильность решения задания.

10. Произведите оценку реальности полученного решения.

11. Запишите ответ.

Пример заданий для промежуточной аттестации:

Планы и методические указания

Задания:

1. Криптоанализ криптограмм методом частотного анализа
2. Криптоанализ криптограмм методом вероятных слов
3. Криптоанализ аддитивных шифров
4. Стеганография и стеганографический анализ изображений
6. Линейный криптоанализ блочных алгоритмов шифрования
7. Дифференциальный криптоанализ блочных алгоритмов шифрования

Вопросы к зачету:

- Правовые аспекты обеспечения информационной безопасности.
- Средства обеспечения информационной безопасности.
- Основные организационные мероприятия в сфере обеспечения информационной безопасности.
- Технические средства обеспечения информационной безопасности.
- Методы и средства защиты от несанкционированного доступа.
- Криптографические методы защиты информации.
- Защита информации в компьютерных сетях.
- Вирусы и обеспечение безопасности от вирусных атак.
- Основные методы криптографического анализа.
- Компьютерная стеганография в контексте обеспечения защиты информации.
- Основные методы стеганографического анализа.
- Методологические основы комплексной системы защиты информации систем искусственного интеллекта.
- Определение состава защищаемой информации.
- Источники, способы и результаты дестабилизирующего воздействия на информацию.
- Каналы и методы несанкционированного доступа к информации.

- Моделирование процессов комплексной системы защиты информации.
- Нормативно-методическое обеспечение систем защиты информации.
- Управление комплексной системой защиты информации.
- Подходы к созданию состязательных примеров.
- Атаки отравление.
- Атаки уклонением.
- Атаки извлечением.
- Атаки с применением порождающих моделей.

Методические рекомендации по написанию рефератов

Общие положения

Цель написания реферата – углубить знания студентов в области избранных направлений дисциплины, расширить навыки самостоятельной научной работы и опыт подготовки курсовых и выпускных работ.

Тема реферата выбирается студентом из числа рекомендуемых преподавателем. Список тем доступен студентам с начала планового срока выполнения задания. Тема может быть предложена и самим студентом, исходя из результатов практики или собственных научных интересов студента.

Реферат выполняется студентом самостоятельно. Каждому студенту выдается индивидуальное задание.

Почему полезен реферат?

Реферат дает объективный обзор области научного знания и принимает во внимание существующие первичные исследования по теме. Оценивая предыдущий вклад в данной области, реферат может предотвратить дублирование исследований, обращает внимание на противоречивые работы, может предложить эффективные новые направления в исследовании. Всесторонний критический обзор не только резюмирует вопрос, но также устраняет ошибки в фактах и концепциях и возбуждает дискуссию, которая приводит к новой исследовательской деятельности.

Темы рефератов

Примерные темы рефератов предлагаются студентам в виде отдельного списка. Реферат по теме, предложенной студентом обязательно согласовывается с преподавателем.

Содержание рефератов

Рекомендуемое содержание реферата:

Введение. Кратко описывается область, относящаяся к теме реферата. Формулируется цель реферата. Объем раздела - не более 0.5 листа А4.

Основная часть. В свободной форме излагаются концепции, формулировки, идеи, мнения и т.п., касающиеся темы реферата. Структура основной части реферата произвольная. Разделы (подразделы) должны быть логически связаны друг с другом. Текст должен быть написан логично, литературным языком, грамотно, иметь чёткий план. Иллюстративные материалы (схемы, рисунки, графики и т.п.) являются большим плюсом реферата.

Нет никакой необходимости приводить в тексте реферата длинные цитаты из используемых источников.

Ссылки на использованную литературу в тексте реферата обязательны. Объем основной части – от 6 до 8 листов формата А4.

Заключение. Формулируются основные выводы, вытекающие из содержания реферата. Объем раздела - не более одного листа.

Список использованной литературы. Список использованной литературы приводится в конце реферата. Должен содержать не менее 5 наименований источников, изданных за последние пять лет. Ссылки на литературу, включая источники в Интернет, должны быть оформлены в соответствии с действующими стандартами.

Работа над рефератом

В ходе работы над рефератом необходимо:

Подобрать необходимую для разработки темы литературу (научную, практическую, справочную, информационную, документальную и т.п.). Если необходимо, обратиться за помощью к преподавателю.

Провести критический анализ изученной литературы.

Логично изложить результаты проведённого анализа.

Сроки выполнения и процедура получения оценки

Рефераты выполняются в сроки, определяемые учебным планом. Преподавателю предоставляется электронная копия текста реферата с титульным листом, оформляемые установленном в вузе образом.

Защита студентом реферата производится в установленном порядке в ходе зачета (экзамена) при личном собеседовании с преподавателем. Студент обязан ответить на любой вопрос преподавателя, касающийся содержания представленного реферата.

Положительная оценка реферата предполагает высокий уровень требовательности к его содержанию. Она должна свидетельствовать о достаточно высокой теоретической подготовке и о наличии у автора необходимых знаний по разрабатываемой теме.

Реферат получивший неудовлетворительную оценку, переделывается в установленные сроки.

Требования к рейтинг-контролю

Важной составляющей данного раздела РПД являются требования к рейтинг-контролю с указанием баллов, распределенных между модулями и видами работы обучающихся.

Максимальная сумма баллов по учебной дисциплине, заканчивающейся зачетом, по итогам семестра составляет 100 баллов (50 баллов - 1-й модуль и 50 баллов - 2-й модуль).

Студенту, набравшему 40 баллов и выше по итогам работы в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший до 39 баллов включительно, сдает зачет.

Распределение баллов по модулям устанавливается преподавателем и может корректироваться.

№ модуля	Содержание модулей: наименование разделов и тем	Форма контроля	Нормы оценки работ студентов
1	Основные положения	Компьютерный тест	**5-10**
2	Формальные модели шифров	Компьютерный тест	**5-10**
3	Оценка стойкости блочных шифров Шифр Rijndael (AES)	Компьютерный тест	**5-10**
		Задание на практическом занятии	**5-10**
4	Распределение симметричных ключей	Задание на практическом занятии	**5-10**
5	Криптографические хеш-функции	Задание на практическом занятии	**25-50**
6	Схемы открытого шифрования и их стойкость	Задание на практическом занятии	**5-10**
7	Двухключевые криптосистемы Схемы цифровой подписи и их стойкость	Компьютерный тест	**5-10**
		Задание на практическом занятии	**5-10**
8	Безопасность сети	Компьютерный тест	**5-10**
		Задание на практическом занятии	**5-10**
9	Введение в тему атак на модели машинного обучения	Задание на практическом занятии	
10	Схемы атак	Задание на практическом занятии	

№ модуля	Содержание модулей: наименование разделов и тем	Форма контроля	Нормы оценки работ студентов
11	Атаки на системы искусственного интеллекта	Задание на практическом занятии	
	Итого по модулю 2		**25-50**
	Всего баллов		**50-100**

VII. Материально-техническое обеспечение

Для аудиторной работы

Компьютерный класс № 4в (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Компьютер, экран, маркерная доска, проектор, кондиционер.

Для самостоятельной работы

Помещение для самостоятельной работы обучающихся: Компьютерный класс факультета прикладной математики и кибернетики № 4б (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Компьютер, экран, проектор, кондиционер.

VIII. Сведения об обновлении рабочей программы дисциплины

№ п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			
3.			
4.			
5.			
6.			