Рабочая программа дисциплины (модуля)*
Основы защиты данных в интеллектуальных системах

Направление подготовки (специальность)

01.03.02 Прикладная математика и информатика

Направленность (профиль)

Прикладная математика и искусственный интеллект

Присваиваемая квалификация (степень)

бакалавр

Форма обучения

очная

Год(ы) набора 2024

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2023 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины: получение основных представлений об использовании криптографических методов, основанных на базе алгебры и теории чисел, для защиты данных в интеллектуальных системах.

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-1.1. Выбирает современные технологии и системы искусственного интеллекта для решения задач в профессиональной деятельности.

УК-1.2. Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учетом требований информационной безопасности.

УК-1.3. Применяет и адаптирует правовые и этические нормы и национальные и международные стандарты в области искусственного интеллекта и смежных областях для решения задач в профессиональной изменения социально-экономических условий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.20

2.1 Требования к предварительной подготовке обучающегося:

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Современные технологии разработки программных систем искусственного интеллекта

Анализ требований и проектирование систем искусственного интеллекта

Технологическая (проектно-технологическая) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-91: Способен планировать и организовывать свою деятельность в цифровом пространстве с учётом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности

Знать:

– цели, задачи и предмет, основные понятия информационной безопасности;
– информационные угрозы, их классификацию,;
– возможные последствия для организаций различных форм собственности;
– критерии оценки защищённости информационных систем и систем искусственного интеллекта.

Уметь:

– сознавать опасности и угрозы, возникающие в профессиональной деятельности и в социальной сфере;
– соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.

Владеть:

– навыками работы с информацией с учётом требований информационной безопасности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные криптографические методы для защиты данных в интеллектуальных системах.
3.2	**Уметь:**
3.2.1	– уметь решать типовые задачи;
3.2.2	– уметь использовать математический аппарат для решения теоретических и прикладных задач криптографии;
3.2.3	– уметь организовывать защиту данных в интеллектуальных системах.
3.3	**Владеть:**
3.3.1	– владеть основными математическими понятиями курса.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 64 самостоятельная работа : 37,5 : контактная работа: 70,5 ИКР: 6,5	Виды контроля в семестрах: зачеты с оценкой 4

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Организация защиты данных в интеллектуальных системах			
1.1	Общая характеристика средств и методов защиты данных в интеллектуальных системах /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Основные принципы и модели защиты информации /Лек/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Стеганография. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Псевдослучайные последовательности. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Коллизии хэш-функций. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Программные средства криптографии. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Классические шифры			
2.1	Криптостойкость. Стандартные атаки. /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Классические шифры. /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Моноалфавитные шифры. /Лаб/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.4	Полиалфавитные шифры. /Лаб/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.5	Изучение лавинного эффекта в симметричных алгоритмах шифрования. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 3. Симметричные криптосистемы			
3.1	Группы в симметричных криптосистемах. /Лек/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

3.2	Сеть Фейстеля. SP-сеть. Лавинный эффект. /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Метод вероятных слов. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.4	Полный перебор. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 4. Введение в теорию чисел			
4.1	Арифметика целых чисел. НОД. Алгоритм Евклида. /Лек/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Линейные диофантовы уравнения. Вычеты. Инверсии. /Лек/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.3	Простые числа. Функция Эйлера. /Лек/	4	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.4	Линейное сравнение. Квадратичное сравнение. Символ Лежандра. /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.5	Простые числа. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.6	Символы Лежандра. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.7	RSA. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.8	Дискретное логарифмирование. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.9	Алгоритм Рабина. /Лаб/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 5. Эллиптическая криптография			
5.1	Эллиптическая криптография /Лек/	4	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 6. Иная контактная работа			
6.1	Выполнение семестровой работы /Ср/	4	20	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
6.2	Подготовка к зачету /Ср/	4	17,5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
6.3	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	4	6,5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Лабораторная работа

Семестровое задание
Вопросы к зачету с оценкой

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Примеры заданий находятся в приложении.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Основы защиты информации.
1. Современная компьютерная система.
2. Исторические подходы к защите информации.
3. Принципы защиты информации.
4. Общая характеристика средств и методов защиты информации в компьютерных системах.
5. Стандартные атаки. Полный перебор.

Классические шифры (оценки криптостойкости).
1. Исторические этапы развития криптографии.
2. Шифр Цезаря.
3. Полибианский квадрат.
4. Одиночная перестановка по ключу.
5. Шифрование методом двойной перестановки.
6. Магические квадраты.
7. Шифр перестановки «скитала».
8. Шифр Виженера.
9. Таблица Трисемуса.
10. Шифр Плейфера.
11. Шифр двойного квадрата.
12. Система омофонов.
13. Шифр Хилла.
14. Роторные машины.

Криптосистемы с закрытым ключом.
1. Моно- и полиалфавитные подстановки.
2. Перестановки.
3. Гаммирование. Датчики псевдослучайных чисел.
4. Абсолютная криптостойкость.
5. Сеть Фейстеля. SP-сеть.
6. Алгоритм ГОСТ 28147-89. Режимы шифрования. Криптосистемы с открытыми ключами
1. Алгоритм Меркла-Хеллмана.
2. Алгоритм Рабина.
3. Алгоритм RSA.
4. Алгоритм шифрования Эль-Гамаля.
5. Алгоритм Диффи-Хеллмана.
6. Алгоритм Диффи-Хеллмана для эллиптических кривых.
7. Алгоритм шифрования на основе эллиптических кривых.
8. Алгоритм ГОСТ Р 34.10-2012.

Математические основы криптографии
1. Алгоритм Евклида. Расширенный алгоритм Евклида.
2. Линейный диофантовы уравнения.
3. Группы. Теорема Лагранжа. Кольца. Поля.
4. Вычеты. Обратные элементы по сложению и умножению.
5. Линейные сравнения с одним неизвестным.
6. Простые числа. Решето Эратосфена.
7. Алгоритм быстрого возведения числа в степень по модулю.
8. Малая теорема Ферма.
9. Теорема Эйлера.
10. Проверка числа на простоту. Алгоритм AKS. Тест Ферма. Тест квадратным корнем.
11. Алгоритм Миллера Рабина.
12. Основная теорема арифметики. Метод проверки делением. Метод Ферма.
13. Р — 1 метод Полларда, р-метод Полларда.
14. Китайская теорема об остатках.
15. Сравнения второй степени по простому модулю. Критерий Эйле-ра. Символ Лежандра.
16. Дискретный логарифм. Первообразные корни.
17. Алгоритм больших и малых шагов.

18. Алгоритм дискретного логарифмирования Полига-Хеллмана.
19. Эллиптические кривые.
20. Эллиптические кривые в конечных полях.

6.4. Критерии оценивания

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.
Прохождение контрольных мероприятий промежуточной аттестации не обязательно. Зачет проводится по билетам. В билете два вопроса. Билет выбирается случайным образом. Студенту дается 30 минут на подготовку. После этого он рассказывает ответы на вопросы билета. Студенту задается дополнительный вопрос по каждому вопросу.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Сергеева Ю. С.	Защита информации: конспект лекций: учебное пособие (https://biblioclub.ru/index.php?page=book&id=72670)	Москва : А-Приор, 2011	ЭБС
Л1.2	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов (https://urait.ru/bcode/511998)	Москва : Юрайт, 2023	ЭБС
Л1.3	Игнатьев Е. Б.	Защита информации: криптоалгоритмы хеширования: учебное пособие для вузов (https://e.lanbook.com/book/311792)	Санкт- Петербург : Лань, 2023	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Шаньгин В. Ф.	Защита информации в компьютерных системах и сетях (http://e.lanbook.com/books/element.php? pl1_cid=25&pl1_id=3032)	Москва : ДМК Пресс, 2012	ЭБС
Л2.2	Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю.	Криптографическая защита информации: учебное пособие (https://znanium.com/catalog/document?id=416723)	Москва : Издательский Центр РИОР, 2023	ЭБС
Л2.3	Внуков А. А.	Основы информационной безопасности: защита информации: учебное пособие для спо (https://urait.ru/bcode/518006)	Москва : Юрайт, 2023	ЭБС

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, лабораторные занятия и самостоятельная работа студента.
На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На лабораторных занятиях рассматриваются варианты решения теоретических и прикладных задач криптографии.
Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.
1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток»

А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.
Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.
Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).
В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:
а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);
б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);
в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

Приложение 1.
Пример лабораторной работы

ЛАБОРАТОРНЫЕ РАБОТЫ

Лабораторные работы выполняются в бригадах. В каждую бригаду могут входить не более двух студентов. Сдача лабораторной работы в срок, означает сдачу на следующем занятии после занятия, на котором лабораторная работа была выдана. Сдача лабораторной работы возможна и на последующих занятиях, но с обязательным устным ответом на дополнительные вопросы по теоретической части лабораторной работы.

1. Криптоанализ моноалфавитного шифра

Одним из простейших шифров подстановки является моноалфавитный шифр. Рассмотрим исходное сообщение M, пусть оно составлено из символов алфавита $\mathcal{A}$. Тогда моноалфавитным шифром называется отображение $\mathcal{A} \to \mathcal{A}$. Ключом для этого шифра является отображение $\mathcal{A} \to \mathcal{A}$.

Особенностью моноалфавитного шифра является сохранение частотных характеристик символов исходного текста в шифротексте. Этим можно воспользоваться для проведения криптоатаки. Предположим, что исходный текст является текстом на естественном языке. В естественных языках частоты встречаемости символов очень неравномерны. Поскольку моноалфавитный шифр не изменяет частот встреч символов, то сопоставляя частотную таблицу для эталонного текста и шифротекста у нас есть возможность сделать предположения о ключе шифра.

Необходимо отметить, что если объем эталонного текста для нас может быть не ограничен, то объем шифротекста всегда ограничен. Поэтому при построении частотной таблицы у нас неизбежно возникают погрешности в вычислении оценок частот встреч букв. При больших частотах встречи букв это будет менее значимо, поскольку статистики будет хватать для верного упорядочивания букв шифротекста, на редковстречаемых символах – ошибка может значительно искажать картину. Поэтому расшифровав самые часто встречаемые буквы с помощью частотного анализа необходимо использовать дополнительную информацию для криптоанализа остального текста.

Задание на лабораторную работу

С помощью метода частного криптоанализа восстановить исходный текст шифрограммы, зашифрованной моноалафитным шифром.

Порядок действий

1. Выбрать шифротекст для своего варианта (номера бригады).
2. Сформировать частотную таблицу для эталонного текста на русском языке.
3. Сформировать частотную таблицу для шифротекста.
4. Сопоставить частотные таблицы расшифровать пробел в исходном тексте.
5. Перебирая различные варианты расшифровки частовстречаемых символов в исходном тексте на основе частотных таблиц провести частичную дешифровку специфичных слов русского языка (короткие предлоги, местоимения, окончания слов и т. д.).
6. Подбором расшифровать оставшиеся редковстречаемые символы в шифротексте.
7. Подготовить, сдать и защитить отчет.

Содержание отчета

1. Номер бригады и её состав с указанием полных ФИО, номера группы.
2. Дата выполнения лабораторной работы.
3. Тема лабораторной работы и ее номер.
4. Шифротекст.
5. Сопоставленные частотные таблицы для эталонного текста и шифротекста.
6. Ключ моноалавитного шифра.
7. Расшифрованный исходные текст.
8. Если была разработана программа, то ее листинг.

Контрольные вопросы

1. Сколько всевозможных ключей для моноалфавитного шифра с алфавитом $\mathcal{A}$?
2. Насколько неравномерны частоты встреч символов на искусственном языке (например, программный код на языке C/C++)?
3. В чем заключается сложность оценивания частоты встречи редковстречаемых символов в шифротексте?
4. Приведите примеры моноалфавитных шифров.
5. Выделите самый криптостойкий из моноалфавитных шифров.
6. Есть ли заведомо слабые ключи в моноалфавитных шифрах?

Приложение 2.
Контрольные вопросы к зачету с оценкой

КОНТРОЛЬНЫЕ ВОПРОСЫ

Основы защиты информации.

1. Современная компьютерная система.
2. Исторические подходы к защите информации.
3. Принципы защиты информации.
4. Общая характеристика средств и методов защиты информации в компьютерных системах.
5. Стандартные атаки. Полный перебор.

Классические шифры (оценки криптостойкости).

1. Исторические этапы развития криптографии.
2. Шифр Цезаря.
3. Полибианский квадрат.
4. Одиночная перестановка по ключу.
5. Шифрование методом двойной перестановки.
6. Магические квадраты.
7. Шифр перестановки «скитала».
8. Шифр Виженера.
9. Таблица Трисемуса.
10. Шифр Плейфера.
11. Шифр двойного квадрата.
12. Система омофонов.
13. Шифр Хилла.
14. Роторные машины.

Криптосистемы с закрытым ключом.

1. Моно- и полиалфавитные подстановки.
2. Перестановки.
3. Гаммирование. Датчики псевдослучайных чисел.
4. Абсолютная криптостойкость.
5. Сеть Фейстеля. SP-сеть.
6. Алгоритм ГОСТ 28147-89. Режимы шифрования.

Криптосистемы с открытыми ключами

1. Алгоритм Меркла-Хеллмана.
2. Алгоритм Рабина.
3. Алгоритм RSA.
4. Алгоритм шифрования Эль-Гамаля.
5. Алгоритм Диффи-Хеллмана.
6. Алгоритм Диффи-Хеллмана для эллиптических кривых.
7. Алгоритм шифрования на основе эллиптических кривых.

8. Алгоритм ГОСТ Р 34.10-2012.

Математические основы криптографии

1. Алгоритм Евклида. Расширенный алгоритм Евклида.
2. Линейный диофантовы уравнения.
3. Группы. Теорема Лагранжа. Кольца. Поля.
4. Вычеты. Обратные элементы по сложению и умножению.
5. Линейные сравнения с одним неизвестным.
6. Простые числа. Решето Эратосфена.
7. Алгоритм быстрого возведения числа в степень по модулю.
8. Малая теорема Ферма.
9. Теорема Эйлера.
10. Проверка числа на простоту. Алгоритм AKS. Тест Ферма. Тест квадратным корнем.
11. Алгоритм Миллера—Рабина.
12. Основная теорема арифметики. Метод проверки делением. Метод Ферма.
13. $P-1$ метод Полларда. ρ-метод Полларда.
14. Китайская теорема об остатках.
15. Сравнения второй степени по простому модулю. Критерий Эйлера. Символ Лежандра.
16. Дискретный логарифм. Первообразные корни.
17. Алгоритм больших и малых шагов.
18. Алгоритм дискретного логарифмирования Полига-Хеллмана.
19. Эллиптические кривые.
20. Эллиптические кривые в конечных полях.

Рабочая программа дисциплины (модуля)*
Основы защиты данных в интеллектуальных системах
Направление подготовки (специальность)
01.03.02 Прикладная математика и информатика
Направленность (профиль)
Прикладная математика и искусственный интеллект
Присваиваемая квалификация (степень)
бакалавр

Рабочая программа дисциплины (модуля) одобрена и рекомендована:

Проректор по учебной работе	утверждено	В.Е. Федоров

Ученым советом математического факультета

Протокол заседания № 3 от 19.10.2023

Председатель Ученого совета математического факультета	согласовано	Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 3 от 12.10.2023

Заведующий кафедрой	согласовано	А. Н. Ручай
Автор (составитель)		А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1