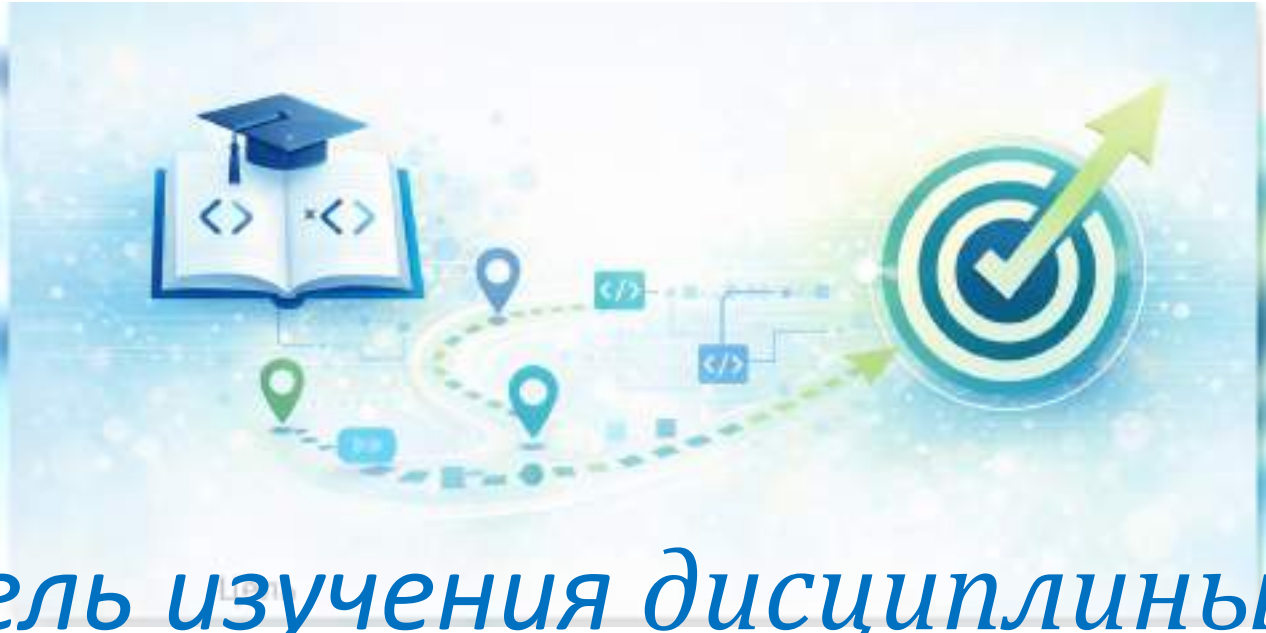
Лекция : Информация и ее измерение

Дисциплина: Основы кодирования
ОП: Системы информационной безопасности

Авторы: Ассоц. проф. КиИИ Даненова Г.Т.
Ассоц. проф. КиИИ Коккоз М.М.
Ассоц. проф. КиИИ Кан О.А.
Ассоц. проф. СМиТ Ахметжанов Т.Б.



Цель изучения дисциплины

- ✓ *Понять природу информации*
- ✓ *Освоить принципы кодирования*
- ✓ *Научиться оценивать эффективность кодов*

В рамках дисциплины решаются следующие задачи:

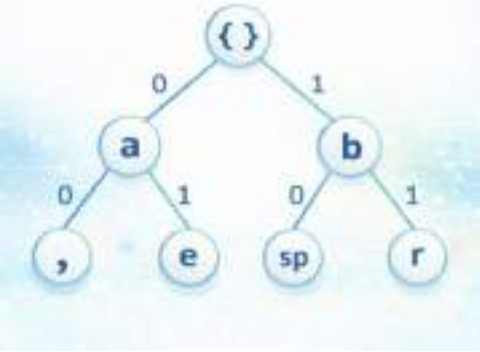
- изучение принципов представления информации в цифровых системах;
- освоение методов количественной оценки информации;
- анализ источников сообщений и их статистических характеристик;
- изучение простейших, неравномерных и статистических методов кодирования;
- освоение алгоритмов Шеннона–Фано и Хаффмана;
- формирование навыков оценки эффективности кодов по длине, энтропии и избыточности;
- развитие умений применять методы кодирования в прикладных задачах IT.

От информации к кодированию: содержание курса

Рассматривается полный цикл работы с информацией — от описания и измерения неопределённости до построения эффективных кодов.

Изучаются принципы представления информации в технических системах, оценка её объёма и избыточности, а также влияние выбора способа кодирования на эффективность хранения и передачи данных.

Курс формирует инженерное понимание того, почему данные кодируются определённым образом, какие теоретические ограничения существуют и как они проявляются в реальных системах.



Основные разделы дисциплины

1. Вероятностные модели источников информации
2. Количество информации и энтропия как меры неопределённости
3. Свойства и характеристики информационных источников
4. Равномерные и простейшие методы кодирования
5. Неравномерное и статистическое кодирование
6. Эффективность и избыточность кодов
7. Алгоритмы Шеннона–Фано и Хаффмана

Энтропия задаёт “цену” данных: она показывает, где в сообщении есть закономерность (сжимаемость), а где — чистая случайность (несжимаемый остаток).

Код — это компромисс между ресурсами и надёжностью: выбирая способ кодирования, мы управляем длиной сообщения, скоростью передачи и устойчивостью к ошибкам в канале.

«Минимум бит» — это нижняя граница сжатия: он показывает, сколько информации в данных неизбежно остаётся и ниже какого объёма сжать уже нельзя без потерь.

Практико-ориентированность дисциплины

реализуется через *лабораторные работы*, в которых студенты:

- формируют источники сообщений на основе реальных данных;
- вычисляют вероятности, энтропию и избыточность;
- строят и сравнивают различные виды кодов;
- реализуют методы кодирования программно;
- анализируют эффективность различных подходов

Итогом изучения дисциплины является курсовая работа, в рамках которой студент выполняет полный цикл анализа источника информации и построения оптимального кода с обоснованием выбора метода.

В результате обучения студент умеет:

- рассматривать кодирование как инженерный способ представления информации;
- анализировать влияние выбора кодов на эффективность хранения и передачи данных;
- оценивать предельные возможности и ограничения информационных систем;
- сравнивать различные способы кодирования по критериям эффективности и избыточности;
- использовать кодирование как инструмент оптимизации информационных процессов.

Теория кодирования лежит в основе:

- компьютерных сетей и телекоммуникаций;
- систем хранения и сжатия данных;
- мультимедийных технологий;
- криптографии и информационной безопасности;
- обработки сигналов, изображений и видео;
- встроенных, интеллектуальных и распределённых систем.

Понимание принципов кодирования необходимо специалистам в области программирования, сетевых технологий, анализа данных, кибербезопасности, системного проектирования и разработки цифровых платформ.

Кибербезопасность

Кибербезопасность – это реализация мер по защите информационных систем, компьютерных сетей и программ от хакерских атак.
Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.
Число информационных систем, подверженных атакам, возрастает с увеличением их количества.

Для обеспечения информационной безопасности используется целый комплекс мер, включая защиту от пожаров, наводнений и других природных катаклизмов, обучение персонала по работе с информацией, физическое ограничение доступа к серверам и другим важным элементам информационной инфраструктуры, законодательные меры защиты и др.
Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как злоумышленники становятся все более изобретательными.

Методы защиты информационных систем принято делить на три основные категории.

Физические методы защиты образуют внешний уровень защиты. Сюда можно отнести службу охраны учреждения, проверяющей документы на входе.

К физическим методам защиты также относятся меры защиты от пожаров, скачков напряжения электропитания, наводнений и других техногенных опасностей.

Всевозможные датчики, видеокамеры, электронные замки, установленные на охраняемых помещениях также относятся к физическим методам защиты.

Организационно- правовые методы предназначены для формирования общей политики безопасности учреждения и включают воспитательные меры защиты, которые призваны воспитывать у сотрудников чувство ответственности за свою работу, работу коллектива и предприятия в целом, информировать служащих о мерах наказания, предусмотренных за те или иные нарушения, а также специальные процедуры принятия и увольнения сотрудников.

К техническим методам защиты относятся программно-аппаратные средства защиты, осуществляющие процедуры аутентификации и идентификации пользователей, защиту данных от несанкционированного доступа, криптографические средства защиты, а также средства безопасной передачи и приема данных по компьютерным сетям, защиту от вирусов, хакерских атак и т.п.

Типы угроз кибербезопасности

Вредоносное программное обеспечение – это такое программное обеспечение, в результате действия которого в компьютерной системе осуществляются непредусмотренные пользователем действия, наносящие вред владельцу информации или другим субъектам.

Вредоносное программное обеспечение предназначено для получения несанкционированного доступа к ресурсам компьютерной системы.

Признаками заражения компьютера вредоносным ПО считаются: автоматическое открытие окон с незнакомым содержимым, частое зависание компьютера, появление системных сообщений об ошибке и др.

К вредоносному программному обеспечению относятся:

- компьютерные вирусы (Vuruses);
- программы вымогатели;
- сетевые черви (Worms);
- троянские программы (Trojans);
- программы-шпионы (Spy Ware);
- другие программы, наносящие вред ПК.

Компьютерный вирус – программа (или сегмент кода), которая может присоединяться к другим программам и файлам, способная приводить к нарушению целостности и доступности информации путем ее уничтожения, модификации или блокирования, а также вызывать снижение эффективности работы или повреждение компьютерной системы.

Компьютерные вирусы могут распространять свои копии по ресурсам локального компьютера с целью последующего запуска своего кода при каких-либо действиях пользователя.

Классификация вирусных программ

Вирусы классифицируются по следующим признакам:

- По воздействию на ИС;
- По способу заражения;
- По среде обитания;
- По особенностям алгоритма.

По воздействию все вирусы можно разделить на:

Безвредные вирусы. Они не мешают работе компьютера, но могут уменьшать объем свободной оперативной памяти и памяти на дисках.

Опасные вирусы. Такие вирусы могут привести к определенным сбоям в работе операционной системы.

Очень опасные вирусы. Эти вирусы могут уничтожить данные, находящиеся на жестком диске, вывести из строя операционную систему и т. д.

По способу заражения вирусы можно разделить на:

Резидентные вирусы. Резидентный вирус при заражении компьютера находится в оперативной памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают оперативную память компьютера и являются активными ограниченное время.

По среде обитания вирусы можно разделить на:

Файловые вирусы. Распространяются путем внедрения своего кода в тело исполняемых файлов.

Загрузочные вирусы. Заражают загрузочный сектор винчестера.

По особенностям алгоритмов все вирусы можно разделить на:

Стелс-вирусы. Это вирусы, которые умеют скрывать свое присутствие в системе.

Полиморфные вирусы. Особенностью этих вирусов является умение изменять собственный код, чтобы ввести в заблуждение антивирусные программы.

Троянские вирусы. Это вредоносные программы, стирающие информацию на вашем компьютере. маскируют свои действия под видом выполнения обычных приложений.

Интернет черви. Это вирусы, которые распространяются по глобальным сетям, поражая целые системы. Почтовые вирусы, самые опасные из них.

Backdoor вирусы. Это программы способные предоставлять права удаленного доступа к вашему компьютеру третьим лицам.

Кейлоггер (keylogger) — это регистратор нажатий клавиш. Основным назначением которого является скрытый мониторинг нажатий клавиш и ведение журнала этих нажатий.

Безопасность данных в интерактивной среде

Интерактивные среды (электронная почта, компьютерные сети, Интернет) наиболее уязвимы с позиций безопасности данных.

Одной из главных проблем в Интернете является безопасность данных. Например, злоумышленник в Интернете может получить номер вашей кредитной карточки. Хакер может при помощи Java апплетов и JavaScript приложений, встроенных в HTML документ, взломать машину пользователя.

При работе с электронной почтой нужно придерживаться следующих правил:
- нельзя запускать программы, полученные по электронной почте. Необходимо сохранить файл на диске, проверить его антивирусной программой и только затем запускать;
- запрещается сообщать свой пароль и личные данные;
- при открытии полученных файлов MC Office следует по возможности не использовать макросы;
- важно применять проверенные, а также более новые версии почтовых программ.

Распространение телекоммуникационных технологий в сфере платежных систем увеличивает риски потери информации в звене пользователь - информационная система.

Если добавить к этому распространение мобильной связи, то получается весьма обширное поле для хакеров, ставящих своей задачей получение конфиденциальной информации.

Эффективным средством борьбы с подобного рода рисками является увеличение ответственности и компетентности сотрудников, работающих с ИС.

При разработке эффективной защиты информационных систем должны быть поставлены следующие цели:

- обеспечить **конфиденциальность** данных в ходе их хранения, обработки или передаче по каналам связи;
- обеспечить **целостность** данных в ходе их хранения, обработки или при передаче по каналам связи.
- обеспечить **доступность** данных, хранимых в локальных вычислительных сетях.

41

Конфиденциальность данных

Защита коммерческих секретов напрямую влияет на конкурентоспособность фирмы и её устойчивость на рынке. Здесь информационная безопасность сталкивается с внешними и внутренними угрозами, направленными на хищение данных.

Хакеры, промышленный шпионаж и утечка информации по вине собственных сотрудников представляют наибольшую угрозу.

42

Целостность данных

Сегодня вся коммерческая информация, бухгалтерские данные, финансовая отчетность, планы и т.д., хранятся в локальной компьютерной сети.
В таких условиях информационная безопасность предусматривает систему мер, которые призваны обеспечить надежную защиту серверов и рабочих станций от сбоев и поломок, ведущих к уничтожению информации или её частичной потере.

Доступность данных

Все меры обеспечения информационной безопасности бесполезны, если они затрудняют работу легитимных пользователей.

Обеспечение доступности предполагает, что обладающий соответствующими правами пользователь, субъект или процесс может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не ожидая дольше заданного промежутка времени.

Таким образом, составляющими информационной безопасности являются:

- определение объектов, на которые могут быть направлены угрозы;
- выявление существующих и возможных угроз;
- определение возможных источников угрозы;
- оценка рисков;
- методы и средства обнаружения враждебного воздействия;
- методы и средства защиты от известных угроз;
- методы и средства реагирования при инцидентах.

Следующая лекция

Вредоносное программное обеспечение:
виды и особенности