Клод Шеннон

Работа Клода Шеннона «Теория связи в секретных системах» (1945) с грифом «секретно», которую рассекретили и опубликовали в 1949 году, послужила началом исследований в теории кодирования и передачи информации, и, по всеобщему мнению, придала криптографии статус науки. Именно Клод Шеннон впервые начал изучать криптографию, применяя научный подход. Он определил основные понятия теории криптографии, без которых сейчас она немыслима. Важной заслугой Шеннона является исследования абсолютно секретных систем, и доказательство их существования, а также существование криптостойких шифров, и требуемые для этого условия. Шеннон также сформулировал основные требования, предъявляемые к надежным шифрам.

Статья «Математическая теория связи», была опубликована в 1948 году и сделала Клода Шеннона всемирно известным. В ней Шеннон изложил свои идеи, ставшие впоследствии основой современный теории обработки и передачи информации.

Шеннон ввел понятие информации, содержащейся в передаваемых сообщениях. Развитая им теория помогла решить главные проблемы, связанные с передачей сообщений, а именно: устранить

избыточность сообщений, произвести кодирование и передачу сообщений по каналам связи с шумами. Решение проблемы избыточности подлежащего передаче сообщения позволяет максимально эффективно использовать канал связи.

Но, наверное, самый выдающийся результат Шеннона – это теорема о пропускной способности канала.

Любой канал с шумом характеризуется максимальной скоростью передачи информации, этот предел назван в честь Шеннона. При передаче информации со скоростями, превышающими этот предел, происходят неизбежные искажения данных, но снизу к этому пределу можно приближаться с необходимой точностью, обеспечивая сколь угодно малую вероятность ошибки передачи информации в зашумленном канале.

В 1965 г. Шеннон побывал в России и принял участие в конференции по проблемам вычислительной техники. Тогда же встретился с М. Ботвинником, их объединял общий интерес – разработка шахматных программ для компьютеров. Шахматная партия между ними закончилась на 42 ходу поражением Шеннона, хотя в один момент он имел небольшое преимущество, как отмечали участники этой исторической встречи.

Число Шеннона – минимальное количество неповторяющихся шахматных партий, вычисленное им в 1950 году, которое составляет 10^{120}. Расчеты приведены в работе «Программирование компьютера для игры в шахматы» («*Programming a Computer for Playing Chess*»), опубликованной в марте 1950 года в журнале Philosophical Magazine и ставшей одним из фундаментальных трудов в развитии компьютерных шахмат как дисциплины. В основу вычислений легло предположение о том, что каждая игра длится в среднем 40 ходов и на каждом ходе игрок делает выбор в среднем из 30 вариантов. Для сравнения — количество атомов в наблюдаемой Вселенной составляет по разным оценкам от 4×10^{79} до 10^{81}, то есть в 10^{40} раз меньше числа Шеннона.

Кроме этого, Шеннон вычислил и количество возможных позиций, равняющееся примерно 10^{43}.

Это число, однако, включает также ситуации, не соответствующие правилами игры, и поэтому недосягаемые в дереве возможных ходов. В настоящее время появился ряд работ, уточняющих или даже опровергающих это число.

Наше знакомство с работами Шеннона началось на лекции по теоретическим основам радиотехники с анекдота:

– Вы поднимаете телефонную трубку и слышите: «Але!»

– В этом случае Вы не получаете никакой информации, поскольку Вы и так ожидали услышать это слово.

– Но вот Вы поднимаете трубку, и Вас бьет электрическим током! Вы получили огромное количество информации, поскольку уж вот этого-то Вы точно никак не ожидали!

Так преподаватель с кафедры Основ радиотехники доступно объяснил нам суть математической теории информации Клода Шеннона.

Как и всякая наука, она требовала первоначальной аксиоматики. Эту аксиоматику, предложенную К. Шенноном, все приняли доброжелательно, поскольку аргументация большинству показалась разумной. Она основывалась на теории вероятностей, поэтому Вы, конечно, понимаете, что у нее остались те же проблемы соотношения с физической реальностью, что и у первой, но другого подхода до сих пор не появилось. Опять же, кому такой подход не нравится, может предложить свою систему аксиом.

За основу меры информации Клод Шеннон предложил использовать понятие энтропии источника информации. Здесь, конечно, имеется ввиду своя, информационная энтропия, но она введена по аналогии с обычной, физической энтропией, которая встречается в знаменитой теореме Больцмана.

Назовем величину

$$H = -\sum p_i \log p_i$$

энтропией множества вероятностей $p_1 \ldots p_n$.

Величина H обладает рядом интересных свойств, которые также подтверждают, что она является разумной количественной мерой возможности выбора или мерой количества информации.

1. $H = 0$ тогда и только тогда, когда все вероятности p_i, кроме одной, равны нулю, эта единственная вероятность равна единице. Таким образом, H равна нулю только в случае полной определенности исходного опыта. В противном случае H положительна.

2. При заданном n величина H максимальна и равна $\log n$, когда все p_i равны (следовательно, $p_i = 1/n$). То, что в этом случае неопределенность будет наибольшей, чувствуется также и интуитивно.

Количество информации измеряется в битах. По Шеннону, 1 бит – это информация о событии, имеющем два равновероятных исхода.

Определение Шеннона информации как степени уменьшения информационной энтропии источника очень удобно для теоретиков, но крайне неудобно в инженерной практике. Существует как бы два параллельных мира – мир теоретиков и мир практиков. Практики используют свое определение бита. Бит – это разряд двоичного кода, принимающее одно из двух значений.

«Это было недавно, это было давно...»

Отсчет истории сотового телефона обычно начинают с появления на автомобилях полиции Чикаго радиостанций для связи с полицейским участком. А вот что рассказывает В. Немцов о своих первых опытах радиотелефонии в книге «Незримые пути».

«Он вынул из кармана маленький аппарат, нажал кнопку, прислушался, и из коробочки ясно донесся мелодичный женский голос: «Я слушаю». – «С добрым утром, моя дорогая...» Примерно так описывались будущие достижения радиотехники в старых фантастических романах.

...

Вспоминаю первое решающее испытание. Вся моя работа происходила на даче, поэтому ничего не стоило взять с собой чемодан радиостанции и отправиться в лес, откуда я хотел вызвать город.

Дома оставался аппарат, который питался от сети переменного тока. Около него никого не было. Передатчик включался автоматически от моего вызова, а приемник я включил заранее.

Навстречу мне попадались веселые дачники с цветами, теннисными ракетками, удочками. Надо полагать, что человек, бегущий с чемоданом в лес, вызывал у них некоторое недоумение. Я, конечно, волновался. Через десять минут решится успех упорного, годового труда. Да и сам эксперимент очень интересен. Говорить из лесу, без проводов, с любым абонентом городской сети – ведь это же почти фантастический телефон в кармане! Правда, телефон килограммов на пятнадцать. Но об этом я старался не думать. Это же опытная модель, случайная конструкция. Зачем омрачать радость первого эксперимента!

На берегу маленькой речушки в кустарнике стоит мой аппарат с тонкой спицей антенны. Кому же позвонить?

Нажимаю кнопку вызова. Молчание...

Странно, что когда начинаешь вспоминать первые испытания своих аппаратов, то почему-то помнятся именно эти тревожные минуты, минуты ожидания ответа на твой вызов. Так и сейчас... Наконец слышу громкий голос телефонистки:

– Седьмой!

Путаясь, называю номер своего друга.

Гудки. Низкие, музыкальные, как самая лучшая музыка в мире!

– У телефона, – доносится в трубку.

– Как меня слышно?

– Как? Обыкновенно. Это тебе не радио. Ты дома?

– Нет, в лесу.

– Я тебя серьезно спрашиваю. Откуда говоришь?

– «Из лесу, вестимо».

– Ничего не пойму! Приезжай ко мне.

– Нет, ты приезжай. Прямо в лес. Помнишь место у речки?

Я звонил по очереди всем друзьям, и никто не догадывался, что слышит меня по радио. Даже если бы я стал об этом говорить, никто бы не поверил.

Когда друзья собрались, я рассказал им о том, как разговаривал с ними из лесу.

– У меня здесь в чемодане радиопередатчик и приемник. Включаю передатчик и нажимаю вот эту вызывную кнопку. Сигнал принимается на приемнике, который находится дома. В приемнике стоит реле: при вызове оно включает линию телефонной сети и домашний передатчик. Перед телефонисткой, как обычно, зажигается сигнальная лампочка. Ответ со станции я слышу через свой передатчик и называю номер. Телефонистка это тоже слышит, набирает номер, и далее уже, как обычно, все операции идут по проволоке. Абонент отвечает, его голос передается из моего дома по радио. Такова как будто бы сложная система связи.

Все наперебой начали вызывать город.

Стало уже смеркаться, с реки потянуло холодком. Послышался резкий гудок в телефоне. Это был вызов. Звонили с междугородней станции.

– Не отходите от аппарата, сейчас с вами будет говорить Ленинград.

Друзья сидели, недоверчиво поглядывая друг на друга.

– Как это можно вызвать, да еще из Ленинграда?

– А какая разница? Хоть из Владивостока. Если я могу вызвать, значит и меня тоже. Кстати, не перейти ли нам на опушку леса? Там не так сыро.

– А Ленинград?

– Там и переговорим.

Чемодан в руке, антенна, колыхаясь, задевает за ветки. Провод противовеса скользит по росистой траве.

Стоп! Зарычал гудок вызова. Ставлю аппарат на землю. Ленинград!

– Я слушаю...

Мое знакомство с «морзянкой» и радиоперехватом

Вздрагиваю, когда слышу у кого-нибудь из сотового телефона азбуку Морзе: «три точки – два тире – три точки» - СМС. Очень напоминает сигнал бедствия СОС «три точки – три тире – три точки» (Save Our Souls – Спасите Наши Души).

Когда спешу, вместо русского «ж» часто пишу латинское «v», которые имеют один и тот же код Морзе – «Три точки – тире». Во время приема радиограммы на слух при высоких скоростях выписать букву «ж» просто невозможно!

«Скоростники» на соревнованиях по приему записывать от руки уже не успевают и пользуются пишущими машинками «Ундервуд». Только эти машинки выдерживают боксерский «Хук слева» – процесс перевода каретки. Но и «Ундервуды» после соревнований требуют ремонта.

Морзянку освоил в пятом классе, в шестом впервые вышел в эфир телеграфом на любительской КВ радиостанции UA3KHO, в седьмом классе стал чемпионом Ярославской области по приему и передаче радиограмм среди юношей.

Впервые столкнулся с проблемой радиоперехвата тогда же. Перестраиваясь по диапазону, услышал дальнюю радиостанцию 4X4NZ. Дальнюю станцию от ближней всегда можно отличить по федингу – периодическому замиранию сигнала.

Префикс 4X4 был мне незнаком, а времени смотреть на таблицу соответствия стран и позывных, висевшую на стене, времени не было – вот-вот начнется «пайлаб» - свалка, когда все начнут вызывать необычную станцию, появившуюся в эфире, причем это будут делать даже те, кто ее не принимает, а услышав только твой вызов. В этой свалке мощных сигналов от соседей связаться с корреспондентом уже не удастся.

Я был первым, и успел принять: «Ави Гуревич, Тель-Авив, Израиль», он тоже подтвердил, что принял: «Владимир, Любим Ярославской, Россия». Все потонуло в какафонии морзянки.

Через две недели из ЦРК (Центрального радиоклуба в Москве) пришло письмо о времени моей связи с Израилем и текстом переданного сообщения, а также указание отстранить меня от работы в эфире сроком на полгода, поскольку я нарушил циркуляр ЦРК о запрете любительской радиосвязи с этой страной – в то время был какой-то политический конфликт. QSL-карточку из Израиля, подтверждающую эту радиосвязь, храню до сих пор.

Второй радиоперехват моей передачи произошел в лесу под Петрозаводском. Были зональные соревнования по радиомногоборью, наша команда выполняла упражнение «Работа в радиосети». Я был капитаном команды из трех человек, вся команда рассредоточена по лесу на расстоянии в несколько километров. На поляне брошена плащ-палатка, на ней радиостанция Р-104.

Получил от судьи список частот и текст передаваемых радиограмм.

Сам должен принять две радиограммы из несмысловых букв и цифр. Три неверно принятых знака – «баранка».

Судья нажал на секундомер, и я приступил к передаче текста. Передавать довольно просто – в любой момент можешь махнуть рукой и отогнать тучи комаров. А вот когда принимаешь...

Упражнение заканчивалось вторым кругом и моим приемом цифрового текста. Вдруг через наушники слышу сильный гул и чувствую

ураганный ветер, а боковым зрением (оторваться от приема нельзя) вижу солдат с автоматами, которые бегут ко мне. Удивляться решил потом, и даже мелькнула мысль: «Как хорошо, что комаров нет!»

Это пограничники прилетели на вертолете захватывать запеленгованного «шпиона», поскольку организаторы соревнования перепутали одну из частот, которую мне предложили для радиообмена, не согласовав ее с пограничниками.

Совсем не веселы истории с радиоперехватом переговоров наших военных в «горячих точках», в ряде случаев кончившихся трагически. А ведь перехвата можно избежать, создав необходимую аппаратуру. Из этой книжки Вы поймете, как это можно сделать.