**Лекция за 22.02.2012, часть 1**

***Теоретические основы вопросов, связанных с передачей данных на расстояние. Исторический экскурс.***

Задача передачи данных стояла перед человечеством всегда, начиная с того момента, как человек осознал себя как разумное существо. Причин тому очень много: и исторических, и психологических, и иных. Например, одно из определений человека как разумного существа звучит как существо, которое поддерживает развитую систему коммуникаций. Этими коммуникациями и будем заниматься. Они возникли не так давно: задача передачи данных в форме, отличной от устной и письменной речи, появилась примерно 300 лет назад в первую очередь в связи с возникновение военной техники и массовых армий. В качестве примера можно привести ***солнечный телеграф*** в Европе. Его возникновение сказалось на том, что стала появляться отрасль теории кодирования, или теории представления данных (она-то и лежит в основе современных IT). Самый простой пример солнечного телеграфа – это солнечный «зайчик», которым можно подсветить кому-нибудь в окно.

Более сложный способ построения солнечного телеграфа: устанавливаем зеркало (гелиограф) на высокой башне и смотрим с другой башни на это зеркало через подзорную трубу + используем что-то наподобие азбуки Морзе.

Некоторое развитие солнечного телеграфа – ***семафорный телеграф***: вместо зеркал стал использоваться рычаг, подвешенного в одной точке. Различные положения рычага стали кодировать разные значения символа. В 19-ом веке семафорные телеграфы опутали почти всю Европу.

Дальнейшее развитие связи связано с появлением ***электромеханического*** и ***электромагнитного*** ***телеграфов***. Есть источник тока, есть катушка с током, которая создаёт магнитное поле. Соответственно, взаимодействие этих катушек порождает некоторый слабый переменный ток, который воздействует на стрелку компаса или другой индикатор. Таким образом, можно с некоторой разумной скоростью (несколько символов в секунду) передавать информацию вплоть до букв. А с появлением мощных источников тока (в первую очередь динамо-машин) стало возможным упростить систему и передавать на расстояние сигнал: есть ток или нет тока.

С этим связано и появление ***кода Морзе*** – первого искусственного кода, который обладает свойством переменной плотности, то есть в зависимости от частоты использования буквы количество символов, которое кодирует эту букву, меняется от 3 до 5 (а в русской версии до 6) знаков. Каждая буква кодируется сочетанием точек и тире: для кодирования более часто используемых букв используются 3 символа, для менее часто используемых – 5 символов.

Есть ещё важный код, на котором следует остановиться, – ***код Бодо***. Изобретатель, француз Жан Морис Эмиль Бодо, послужил «прототипом» для современной единицы передачи информации – бод. Код Бодо равномерный: каждый символ алфавита кодируется пятью значениями(0 и 1, т. е. есть ток или нет тока). Соответственно, линия Бодо – пятипроводная (очень большой расход меди). Ещё телеграфы Бодо породили перфоленту: оказалось, что очень удобно записывать код не в виде точек и чёрточек грифеля на бумаге, а в виде проколотых отверстий на ленте. Изначально лента Бодо была пятипозиционная, а считыватели перфолент умели работать с пятипозиционной или восьмипозиционной лентой.

**Почему именно 5 позиций?** Это минимальная длина, необходимая для передачи символов английского алфавита. В английском (латинском) алфавите 26 символов: принято считать, что i и j – это один символ, v и w – тоже, так как они похожи по написанию и нет слов, в которых смешивание этих символов приводит к непониманию. Таким образом, из 26 символов остаётся 24 + символы для основных знаков препинания («,», «.», «?», иногда «!») + специальные символы для обозначения начала и конца передачи. Кроме того, клавиатура Бодо была пятиклавишной, то есть можно было работать с одной руки. Рекорды набора символов на такой клавиатуре – 10-15 символов в секунду.

**Генрих Герц** первым написал решения для уравнений Максвелла и сделал важный вывод о том, что электромагнитная энергия может распространяться в пустом пространстве посредством электромагнитных волн (прямое следствие из уравнений Максвелла) и что эти электромагнитные волны можно принять в электрическом контуре и при определенных условиях усилить и наблюдать их в виде неких электрических сигналов. Генрих Герц первым поставил опыты и смог передавать электромагнитное излучение на расстояние 20-30 метров.

Следующий этап беспроводной передачи информации связан с **Поповым** и **Маркони**. В советской литературе приоритет отдаётся Попову, а в зарубежной – ситуация неоднозначна: обычно считают, что Попов первым разработал теорию передачи электромагнитного сигнала на большие расстояния и построил опытный образец, а Маркони запатентовал технологию и наладил серийное производство. На самом деле с Поповым ситуация была довольно-таки проста: по тогдашним законам Российской империи изобретатель не мог запатентовать изобретение за границей, не запатентовав его в России, иначе он лишался на него всех прав, то есть изобретение переходило в казну. А срок патентования в России был очень долгим: в среднем 2-5 лет. Попов, чтобы хоть как-то обеспечить собственный приоритет, опубликовал в журнале русского физико-технического общества описание приёмо-передатчика, указал на необходимость антенны как средства увеличения дальности приёма сигнала (причём указал необходимость антенны неверно). Попов впервые предложил для детектирования радиосигнала использовать нелинейный элемент – **когерер** – металлическая трубочка с железными опилками, которая нелинейным образом меняет своё сопротивление при прохождении электромагнитных волн. Заметим, что любой современный приёмник использует для детектирования электромагнитного сигнала нелинейный элемент.

В дальнейшем радиосвязь очень быстро совершенствовалась, и уже к началу Первой мировой войны почти во всех армиях мира радиопередатчики существовали и активно использовались в боевых действиях.

На самом деле все военные коды до начала 20 века были достаточно примитивны: все использовали примерно один и тот же принцип, существовали **кодовые книги**, которые содержали либо комбинации цифр и букв, либо какие-то конкретные фразы, либо слова, кодирующие те или иные часто встречающиеся в условиях боевых действий фразы. В связи с тем, что боевые действия приняли массовый характер, кодовые книги начали попадать к противникам. Так как замена книг дорогая, то встал вопрос, нельзя ли придумать что-нибудь попроще и получше.

В связи с этим вернулись к тем самым **коммерческим шифрам**, которые были известны ещё с 17-го века. В первую очередь **шифры-подстановки**, когда каждая буква алфавита заменяется любой другой, но они ненадёжны. В конце 19-го – начале 20-го века активно развивалась такая область математики, как теория чисел и абстрактная алгебра, которая в дальнейшем дала развитие всей криптографии.

Во время Первой мировой войны использовали подстановочные шифры, максимально их запутав: составлялась большая подстановочная таблица, в которой каждая буква алфавита заменялась какой-то другой (главное, что однозначно). А если посмотреть в математическую теорию этой науки, то она гласит, что любой такой подстановочный шифр эквивалентен **сдвиговому шифру**, то есть когда весь алфавит сдвигается на некоторую произвольную позицию (например, «а» → «б», «б» → «в» и т.д.). Соответственно, в нетривиальных подстановочных шифрах первая буква замещается с некоторым одним смещением, вторая – с другим, третья – с третьим.

После Первой мировой войны, в 1921 году, некий немецкий учёный изобрёл механическую шифровальную машину, которая потом послужила прототипом **шифровальной машины Enigma** (лучшего шифровального приспособления во время Второй мировой войны). Изобретатель Enigma пытался запатентовать её где угодно, но его изобретением не заинтересовались. Гитлер заинтересовался его изобретением и стал использовать его (изобретение) бесплатно. До сих пор есть закрытые факты, связанные с Enigma. В своё время Англия стала тиражировать машинку и пиарила тему, что код Enigma не раскрываем, несмотря на то, что во время войны английские математики научились этот код считать (1942 год), причём даже был построен механический дешифровщик. До сих пор неизвестно, был ли код Enigma вскрыт в Советском Союзе.