

ИСТОРИЧЕСКИЙ ОЧЕРК

Корифеи теории цифровой связи

Уважаемый читатель! 2008 год для теории цифровой связи можно считать трижды юбилейным. Действительно, 75 лет минуло с 1933 г., когда В.А.Котельников опубликовал фундаментальную теорему, получившую впоследствии его имя; 60 лет назад Клод Шеннон опубликовал свою работу, заложившую основы теории информации; и ровно 50 лет назад А.Г. Зюко сформировал базу современной теории эффективности цифровых телекоммуникационных систем. Эти юбилейные даты послужили поводом для решения редколлегии журнала опубликовать серию очерков, объединенных рубрикой «Корифеи теории цифровой связи» посвященную этим известным ученым. Очерки поручено подготовить члену редколлегии проф. Банкету В.Л. В № 2 журнала «Цифровые технологии» за 2007 год была опубликована статья об академике В.А. Котельникове и его «Теореме отсчетов», в данном журнале читателю предлагается очерк о Клоде Шенноне.

КЛОД ШЕННОН – ОСНОВОПОЛОЖНИК ТЕОРИИ ИНФОРМАЦИИ

БАНКЕТ В.Л.

K. SHANNON – THE FOUNDER OF THE INFORMATION THEORY

V.L. BANKET

Аннотация Излагается роль К. Шеннона в создании теории информации.

Annotation The K.Shannon's role in the creating of the Information Theory is expounding.

Шестьдесят лет тому назад 32-летний инженер-электротехник и математик К. Шеннон опубликовал свою статью «Математическая теория связи», ставшую поворотной вехой в статистической теории связи [1]. Творческий путь К. Шеннона ничем примечательным не выделялся. Математика и наука были его любимыми предметами в школе, а любимым «героем» из области техники был изобретатель Томас Эдисон. С 1932 г. К. Шеннон изучает математику и электротехнику в университете штата Мичиган. Подобная комбинация формальной и прикладной наук привлекала его до конца жизни. В 1936 г. он принят на должность ассистента-исследователя в Массачусетский технологический институт, где работал над методами решения дифференциальных уравнений с использованием анализатора Буша, в котором функции управления осуществлялись релейными цепями. Его коллеги уже тогда знали методы решения задач двоичной логики с помощью реле, но Шеннон скоро пришел к выводу, что подобные задачи удобно решать с применением формальных методов, подобных Булевой алгебре. В 1937 г. Шеннон представляет магистерскую работу «Символический анализ релейных и коммутируемых цепей», которая в последующем оказалась базовой работой по цифровой обработке сигналов, поскольку в ней предлагались регулярные методы, пригодные для анализа и синтеза логических цепей. За эту работу К. Шеннон получил в 1940 г. степень магистра. Последующие 15 лет Шеннон работал в *Bell Laboratories* совместно с такими теоретиками, как *H. Nyquist* и *H. Bode*. В этот период он разработал основы теории информации, опубликованные в 1948 г. в статье «Математические основы теории связи» [1]. К. Шеннон предложил использовать энтропию в качестве меры количества информации. Понятие энтропии использовалось Больцманом в теории термодинамики газов. Несколько ранее Хартли

пытался определять количество информации мерой неопределенности ансамбля [2]. Заслуга К. Шеннона состояла в синтезе в едином понятии «информационная энтропия» подходов Хартли и Больцмана. В последующем оказалось, что определение энтропии было конструктивным, т. е. позволило решить многие задачи статистической теории связи. Примечательно, что работа К. Шеннона направила усилия многих исследователей в нужное русло. Причем, К. Шеннон не решал самостоятельно частные задачи теории, а предоставлял эту работу своим последователям. Многие из коллег и последователей К. Шеннона впоследствии внесли весомый вклад в теорию информации и теорию цифровой связи: Р. Фано (соавтор статистического кода Шеннона-Фано), М. Элайес (автор метода сверточного кодирования), Дж. Мэсси (автор метода порогового кодирования/декодирования). В русскоязычной среде многие также внесли вклад в развитие теории: А.Г. Зюко (автор теории эффективности информационных систем), акад. АН СССР А. Харкевич (монография «Очерки общей теории связи»), чл. корр. АН СССР.

В. И. Сифоров (основатель и первый директор института проблем передачи информации АН СССР). В ВУЗах связи начали преподавать основы теории информации. Мне довелось в период 1960-1975 гг. общаться с акад. Р.Л. Добрушиным, который был ведущим специалистом по теории информации института проблем передачи информации АН СССР и осуществлял редактирование переводов работ К. Шеннона на русский язык. Добрушин отмечал «колоссальную» научную интуицию Шеннона, который предсказывал в личных беседах и на семинарах многие результаты будущих исследований. На основе информационных подходов им также была подготовлена статья «Теория связи секретных систем» [3]. В современных условиях средства телекоммуникаций должны обеспечивать передачу больших объемов информации, гарантируя одновременно и безопасность связи. Вклад К. Шеннона в становление и развитие криптографии общеизвестен. Однако К. Шеннон был не только "крестным отцом" криптографии с секретным ключом. Его основополагающая работа (1949 г.) способствовала превращению криптографии из искусства в науку, когда появилась возможность ввести понятие совершенной секретной системы и теоретически указать способ построения нераскрываемого ключа. Этому способствовало и то, что с точки зрения криптоаналитика секретная система почти идентична системе передачи информации на фоне шума.

Одним из последних расширений теории информации является квантовая теория информации. Нильс Бор отмечал, что "всякий, кто способен рассматривать квантовую механику без головокружения, наверняка ее не понимает". Информационная теория, базирующаяся на квантовых принципах, расширяет и дополняет классическую теорию информации, равно как комплексные числа расширяют и дополняют понятие чисел вещественных. Новая теория содержит квантовые обобщения классических понятий источника, канала и кода, базирующиеся на двух взаимодополняющих видах информации: классической (неопределенность события) и квантовой (неопределенность состояния). В последние десятилетия в компьютерных технологиях наблюдается устойчивая тенденция: каждые два года быстродействие компьютера возрастает вдвое и так же вдвое уменьшаются размеры компонентов. Уже сейчас в обычном компьютере для хранения одного бита информации используется несколько тысяч атомов. Ожидается, что в ближайшем будущем это количество снизится до нескольких десятков, вслед за чем должен произойти переход на квантовые принципы хранения и обработки информации. Полученные в квантовой теории информации результаты пока являются теоретическими. Однако работы в этом направлении развиваются столь стремительно, что в ближайшие годы можно ожидать появления первых прикладных результатов.

ВЫВОДЫ

В заключение, отмечая роль теории информации в развитии техники цифровой связи можно привести слова К. Шеннона, который, вообще говоря, не склонен был к популяризации своих идей. Вместе с тем, он все же выступил в журнале "Fortune" (1953 г.) с оценкой роли теории информации, где писал:

"Большие научные теории, как и известные симфонии или романы являются замечательными и вместе с тем редкими творениями людей. Научные теории отличает от других созданий человечества то, что они способны быстро и кардинально изменить мироощущение людей.. Без преувеличения можно сказать, что прогресс человечества в значительной мере зависит от плодотворных приложений теории информации, в равной мере как энергетика зависит от известных уравнений А. Эйнштейна".

Список использованных документов

1. *K.Shannon*. A mathematical theory of communications//Bell System Techn.Journal.Vol.27,№ 3.1948 pp.379-423; Vol.27,№ 4.1948 pp.623-656.
2. *R.Hartley*.Transmission of information// Bell System Techn.Journal.Vol.7,№ 3.1928 pp.535-563.
3. *K.Shannon*. Communication theory of secrecy systems//Bell System Techn.Journal.Vol.28, № 4.1949 pp.656-715.

