Экз.№ 1.

Основные положения автоматической шифровки.

Рассмотрим основные положения автоматической шифровки сообщений.

Введем ряд терминов.

Сообщением мы будем называть то, что необходимо передать из одного пункта в другой. Таким образом, сообщением можно называть какой-либо знак, отдельную букву, слово, депешу или даже совокупность депеш.

Сигналами мы будем называть совокупность посылок, которые характеризуют передаваемое сообщение и при приеме которых оно становится передаваемым сообщениям установлено.

Число сигналов должно равняться числу возможных сообщений или быть больше этого числа. В дальнейшем мы будем рассматривать передачи, в которых эти числа равны.

Если всегда определенному сообщению соответствует определенный сигнал, при помощи которого это сообщение передается, то такую передачу мы будем называть неизменяющейся передачей.

Действительно, если в этом случае устройство передающей аппаратуры будет известно, а мы будем предполагать тут и в дальнейшем, что это так, то будет известно, какому сообщению какой сигнал соответствует, и по полученным сигналам можно будет однозначно судить о переданных сообщениях.

Шифром мы будем называть закон, связывающий сигналы с соответствующими сообщениями, при "зашифрованной" передаче.

Если одно и то же сообщение может передаваться аппаратурой при помощи различных сигналов, в зависимости от шифра, и шифры могут произвольно меняться, то такую передачу мы будем называть зашифрованной передачей.

19 июня 1941 года - В.А.Котельниковым доказана абсолютная стойкость системы шифрования "бит на бит" (совершенно стойкий по К.Шеннону шифр), то есть доказано, что можно создать математически недешифрируемую систему засекречивания, если каждый знак сообщения будет засекречиваться выбираемым равновероятно знаком шифра.

ОСНОВНЫЕ ПОЛОЖЕНИЯ АВТОМАТИЧЕСКОЙ ШИФРОВКИ

В. А. Котельников

Рассмотрим основные положения автоматической шифровки сообщений.

Введем ряд терминов.

Сообщением мы будем называть то, что необходимо передать из одного пункта в другой. Таким образом, сообщением можно назвать какой-либо знак, отдельную букву, слово, депешу или даже совокупность депеш.

Сигналом мы будем называть совокупность посылок, которые характеризуют передаваемое сообщение и при помощи которых осуществляется передача сообщения на расстояние.

Число сигналов должно равняться числу возможных сообщений или быть больше этого числа. В дальнейшем мы будем рассматривать передачи, в которых эти числа равны.

Если всегда определенному сообщению соответствует определенный сигнал, при помощи которого это сообщение передается, то такую передачу мы будем называть *незашифрованной передачей*.

Действительно, если в этом случае устройство передающей аппаратуры будет известно, а мы будем предполагать тут и в дальнейшем, что это так, то будет известно, какому сообщению какой сигнал соответствует, и по перехваченным сигналам можно будет однозначно судить о передававшихся сообщениях.

Шифром мы будем называть закон, связывающий сигналы с соответствующими сообщениями, при зашифрованной передаче.

Если одно и то же сообщение может передаваться аппаратурой при помощи различных сигналов, в зависимости от шифра, и шифры могут произвольно меняться, то такую передачу мы будем называть *зашифрованной передачей*.

Если одному сообщению при разных шифрах соответствуют всегда различные сигналы, то такие шифры мы будем называть *неповторными*. Если возможен случай, когда при различных шифрах одному сообщению будут соответствовать одинаковые сигналы, то шифры мы назовем *повторными*.

Мы будем считать в дальнейшем, если не будет оговорено обратное, что *устройство аппаратуры и все возможные* при этой аппаратуре *шифры известны* лицам, занятым расшифровкой перехваченных сигналов. Это наихудший случай, и он может иметь место на практике, т. к. производством и эксплуатацией аппаратуры будет занят довольно

большой круг лиц. Кроме того, число методов зашифровки ограничено, и по характеру передаваемых сигналов можно судить о методе шифровки.

Учитывая это, мы разделим все возможные зашифровки на 3 класса.

Зашифровка 3 *класса* («плохая»).

При этой зашифровке по перехваченному сигналу, не зная, какой из шифров применялся, можно установить передававшееся сообщение однозначно.

Зашифровка 2 *класса* («хорошая»).

При этой зашифровке по перехваченному сигналу, не зная, какой из шифров применялся, нельзя однозначно определить, какое сообщение передавалось, но можно выделить из всех возможных сообщений группу сообщений, содержащую передававшееся сообщение.

Зашифровка 1 *класса* («совершенная»).

При этой зашифровке по перехваченному сигналу, не зная, какой из шифров применялся, нельзя ни однозначно определить, какое сообщение передавалось, ни выделить из всех возможных сообщений меньшую группу, содержащую, передаваемое сообщение.

При всех этих определениях предполагалось, что зашифровывающая аппаратура и, значит, все возможные при этой аппаратуре шифры известны лицу, расшифровывающему перехваченные сообщения.

Поясним сказанное простейшими примерами, а также сделаем из этих примеров основные выводы, по которым можно судить, к какому классу относится та или другая шифровка. Эти выводы в дальнейшем мы сформулируем и докажем более точно.

Предположим, что нужно передать одно из пяти сообщений, которые мы назовем. А, Б, В, Г, и Д, так, чтобы по сигналам, которыми эти сообщения будут передаваться, нельзя было бы понять, которое из этих сообщений передано. Предположим, что шифрующее устройство может посылать пять сигналов в зависимости от того, какое сообщение передается и какой шифр применен. Условно назовем эти сигналы а, б, в, г, и д.

Предположим, что сигналы будут определяться в зависимости от шифра и от сообщения, согласно таблице 1.

Разберем ряд случаев.

Случай 1.

Пускай наше устройство может применять лишь три шифра, скажем шифры 1, 2 и 3. Допустим, что был передан сигнал «б». Зная таблицу, можно сказать, что очевидно передавались сообщения А, Г или Д, т. к. в других сообщениях сигнал «б» не применяется. Таким образом, если не точно, то все же приблизительно можно узнать, какое сообщение передавалось. Сделаем из этого вывод.

Таблица 1

Сообщение	№ шифра						
	1	2	3	4	5	6	7
А	а	в	б	д	г	в	в
Б	в	г	а	б	д	г	д
В	г	д	в	а	б	а	б
Г	д	б	г	в	а	б	г
Д	б	а	д	г	в	д	а

Вывод 1. Если число возможных шифров меньше, чем число возможных сообщений, то можно из всех возможных сообщений выделить группу, одно сообщение из которой наверняка передавалось.

Это снижает качество шифровки, т. к. позволяет до некоторой степени судить о сообщении, которое передавалось.

В этом случае мы будем иметь шифровку 2 класса.

Случай 2.

Допустим, что сообщения и шифры остались те же, что и в случае 1, но дополнительно известно, что сообщения Г и Д не могли передаваться (например, эти сообщения в данный момент бессмысленны). Тогда в ряде случаев сообщение может быть расшифровано однозначно. Действительно, если при этом был послан сигнал «б», то наверняка можно сказать по таблице, что передавалось сообщение А; если передавался сигнал «д», то значит сообщение было В.

Вывод 2. Если число возможных шифров меньше, чем число возможный сообщений и, кроме того, ряд сообщений заведомо не передавался, то в ряде случаев сообщения могут быть расшифрованы однозначно.

В этом случае мы имели шифровку 3 класса.

Случай 3.

Допустим, что могут быть использованы пять шифров 1, 2, 3, 4 и 5, причем, как видно из таблицы, любые два из этих шифров не дают при зашифровке одного и того же сообщения одинаковых сигналов.

Таким образом, в этом случае мы имеем число шифров, равное числу возможных сообщений, и эти шифры неповторны.

Как легко видеть в этом случае, при перехвате переданного сигнала совершенно нельзя судить о том, какое сообщение передавалось. Так сигналу «а» могут соответствовать сообщения А, Б, В, Г и Д. То же и остальным сигналам.

В этом случае, даже если известно, что часть сообщений не могла передаваться, все же нельзя будет сказать, какое из возможных сообщений передавались. Так, если сообщения Г и Д заведомо не передавались, то все же по принятому сигналу нельзя будет судить

о том, что было передано из оставшихся сообщений — сообщение А, Б или В, т. к. каждый из сигналов может соответствовать любому из этих сообщений.

Вывод 3. Если число шифров равно числу возможных сообщений и эти шифры неповторные, то по перехваченному сигналу нельзя судить, какое сообщение было передано, если даже известна часть сообщений, которые заведомо не передавались.

В этом случае мы будем иметь совершенную зашифровку 1 класса.

Случай 4.

В выводе 3 специально указывалось, что шифры должны быть неповторные. Действительно, если, например, будут употребляться шифры 3, 4, 5, 6 и 7, которые являются повторными, и будет известно, что сообщения А и Б не передавались, то сигнал «д» будет однозначно указывать, что передавалось сообщение Д.

Следует еще отметить, что после передачи одного сообщения следует для передачи другого сменить шифр. Покажем на примере, что это для совершенной шифровки необходимо.

Случай 5.

Допустим, что применяются шифры 1, 2, 3, 4 и 5. Допустим, что дополнительно известно, что сообщения Д и Г не могли передаваться. Мы видели, что при этом шифровка получается совершенной. Пусть будут переданы сигналы «б» и затем без смены шифра «в». В этом случае по таблице будет легко обнаружить, что использовался шифр № 3, т. к. лишь при этом шифре могут получиться сигнал «в» совместно с сигналом «б» от сообщений А, Б и В. Отсюда сразу видно, что передавались сообщения сначала А, а потом В.

Вывод 4. Для совершенной шифровки необходимо, чтобы шифры менялись с каждым передаваемым сообщением.

Сформулируем теперь полученные выводы более полно и докажем их.

Положение 1.

Пусть число возможных передаваемых сообщений и число сигналов равны N, число шифров равно M. Тогда по перехваченному сигналу, не зная номера шифра, можно выделить из N возможных сообщений группу jM сообщений, в которой будет заключаться переданное сообщение. Здесь:

$j = 1$, если шифры неповторные,

и

$j < 1$, если шифры повторные.

Доказательство.

Каждый сигнал в любом шифре должен соответствовать одному только сообщению, даже зная шифр, нельзя будет однозначно расшифровать сигнал.

Если у нас может применяться M неповторных шифров, то одному сигналу может соответствовать при различных шифрах M различных

сообщений. При повторных шифрах одному сигналу иногда может соответствовать меньше, чем M сообщений, т. к. при различных шифрах сигнал в этом случае может соответствовать одному и тому же сообщению.

Таким образом, перехватывая сигнал, мы можем определить группу сообщений величиной jM, которой этот сигнал будет соответствовать. В этой группе обязательно будет лежать и переданное сообщение. Таким образом, положение 1 доказано.

Положение 2.

Пусть число возможных передаваемых сообщений и число сигналов равны N, число шифров M и, кроме того, что L определенных сообщений не передавалось, причем $L > jM - 1$. Тогда по перехваченному сигналу в ряде случаев можно будет однозначно указать сообщение, которое передавалось, т. е. шифровка будет 3 класса. Здесь:

$j = 1$, если шифры неповторные,

и

$j < 1$, при повторных шифрах.

Доказательство.

По положению 1 по перехваченному сигналу можно выделить группу jM сообщений, в которой будет лежать переданное сообщение.

Если $L = jM - 1$, то может оказаться, что в данной группе из jM сообщений имеются $jM - 1$ сообщений, которые заведомо не передавались, и лишь одно сообщение, которое могло передаваться. Ясно, что в этом случае как раз и передавалось это единственно возможное сообщение.

Положение 3.

Если число возможных передаваемых сообщений N, число шифров M и число используемых сигналов равны между собой и шифры взяты неповторные, то шифровка будет совершенной и нельзя будет по перехваченному сигналу ничего сказать о переданном сообщении, если даже заведомо будет известно, что часть сообщений не передавалась.

Доказательство.

При неповторных шифрах каждый данный сигнал при каждом новом шифре должен соответствовать новому сообщению. Если число шифров M равно числу сообщений N, то каждый сигнал может соответствовать N различным сообщениям, т. е. может соответствовать любому возможному сообщению. Таким образом, по перехваченному сигналу нельзя даже выделить группу, в которой будет содержаться переданное сообщение.

Если будет известно, что L определенных сигналов не могло передаваться, то, на основании этого, число возможных сообщений, которым может соответствовать данный сигнал, упадет до $N - L$. Ясно, что это ничего нового для расшифровки не даст.

Таким образом, положение 3 доказано. Это положение не противоречит также положениям 1 и 2.

Действительно, по положению 1 мы можем выделить группу сигналов, равную M, но так как в нашем случае $M = N$, то в эту группу попадут все возможные сообщения.

По положению 2 сигнал может быть расшифрован однозначно, если

$$L > jM - 1.$$

В нашем случае, если $L = M - 1$, т. е. должно быть известно, что все возможные сообщения, кроме одного определенного, не передавались. Но это условие по существу равносильно тому, что мы заранее знали сообщение, которое будет передаваться.

Положение 4.

Для получения совершенной шифровки при передаче нескольких сообщений нужно шифры чередовать по заранее обусловленному закону, причем, аппаратура должна допускать любой закон чередования шифров.

Доказательство.

Действительно, передачу n сообщений можно рассматривать, как передачу одного комбинированного сообщения, которое может иметь N^n вариантов, где N — число вариантов одного сообщения.

Согласно положению 3, для совершенной шифровки этого необходимо N^n неповторных вариантов шифра.

Если менять шифры отдельных сообщений по какому-то заданному заранее закону, то получится комбинированный шифр, который будет состоять из последовательности n простых шифров. Это будет шифром комбинированного сообщения.

Если закон чередования шифров может быть сделан любым, то мы получим N^n различных вариантов шифра.

Эти шифры будут неповторными. Действительно, два любые, различные комбинированные шифры должны отличаться друг от друга хотя бы в одном из составляющих шифров. В этом случае комбинированные сигналы будут отличаться друг от друга хотя бы в одном из составляющих сигналов, т. к. составляющие шифры были взяты неповторными, а это значит, что комбинированные шифры также будут неповторны.

Таким образом, если применить смену шифров для каждого сообщения, то мы сможем обеспечить условие положения 3-го и этим добиться совершенной шифровки.