ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 31 МАТЕМАТИКИ Выпуск 1
2024

С. И. Серов (Москва, ОПиПМ). **О роли априорных вероятностей сообщений в вопросе о совершенной секретности шифров по Котельникову–Шеннону.**

УДК 519.719.2 DOI https://doi.org/10.52513/08698325_2024_31_1_1

Резюме: Совершенная секретность шифра не зависит от конкретных значений априорных вероятностей сообщений.

Ключевые слова:шифр, совершенная секретность, априорные вероятности.

В 40-х годах XX века в СССР и США Владимир Александрович Котельников ([1]) и Клод Эльвуд Шеннон ([2]) независимо доказали существование и построили теоретически недешифруемый шифр с «латинским квадратом» и одноразовым ключом: В. А. Котельников в отчете от 19 июня 1941 года ([3]), а К. Шеннон в работе 1945 года ([4]).

К.Шеннон применил байесовский подход и определил совершенную секретность в [5, с. 361]:

> «После того как шифровальщик противника перехватил некоторую криптограмму E, он может вычислить, по крайней мере в принципе, апостериорные вероятности различных сообщений $P_E(M)$. Естественно определить *совершенную секретность* с помощью следующего условия: для всех криптограмм апостериорные вероятности равны априорным вероятностям сообщений $P(M)$ **независимо от величины этих последних** (выделено автором). В этом случае перехват сообщения не дает шифровальщику противника никакой информации.»

На этом в вопросе о независимости совершенной секретности от конкретных значений априорных вероятностей сообщений можно было бы поставить точку, но во введении к этой работе сам К. Шеннон ([5, с. 337]) приводит это же определение без выделенных выше слов. Это позволило предположить зависимость совершенной секретности шифра от конкретного вида априорного распределения на множестве сообщений и даже поменять ролями ключ и сообщение (см. книгу [8, с. 46, 47] и ее библиографию).

Криптограмма E есть результат применения к сообщению M преобразования T_K, выбранного из множества однозначных преобразований $\{T_1, \ldots, T_m\}$ в соответствии с используемым ключом K :

$$E = T_K M, K \in \{1, \ldots, m\}, M \in \{M_1, \ldots, M_n\}.$$

Для возможности однозначного расшифрования преобразования должны быть обратимыми. Ключ K и шифруемое сообщение M выбираются независимо в

соответствии с априорными распределениями вероятностей

$$P(K) = \begin{pmatrix} 1 & \dots & m \\ p_1 & \dots & p_m \end{pmatrix} \quad P(M) = \begin{pmatrix} M_1 & \dots & M_n \\ q_1 & \dots & q_n \end{pmatrix}, \tag{1}$$

где вероятности неотрицательны. Равенство какой-либо из них нулю не дает повода исключать соответствующий исход из множества возможных значений, так как эти вероятности могут изменяться. Недопустимо и произвольно добавлять исходы с нулевыми вероятностями. Множества допустимых исходов в (1) задают преобразования $\{T_1, \dots, T_m\}$.

К. Шеннон изображает секретную систему в виде схемы [5, с. 344], на которой каждое сообщение $M \in \{M_1, \dots, M_n\}$ соединяется линией с криптограммой $E = T_k M$ для каждого $k \in \{1, \dots, m\}$. Так строится множество возможных криптограмм $\{E\}$.

В. А. Котельников рассматривает таблицу — у К. Шеннона это матричное представление шифра ([4, p. 30]) — это таблица, в которой на пересечении строки, соответствующей сообщению M, в столбце, соответствующем ключу k, находится $E = T_k M$.

$M \backslash K$	1 … k … m
M_1	
⋮	⋮
M	$E = T_k M$
⋮	⋮
M_n	

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

При заданных множествах преобразований, ключей и сообщений множество возможных криптограмм $\{E\}$ определяется как множество элементов внутри этой таблицы и не зависит от априорного распределения на множестве сообщений.

Вероятность того, что для шифрования выбранного сообщения M_j предварительно независимо был выбран ключ k и получена криптограмма $E = T_k M_j$, равна $p_k q_j$. Поэтому эта вероятность равна:

$$P(M = M_j, K = k, E) = p_k q_j I\{E = T_k M_j\}, \tag{2}$$

где $I\{\cdot\}$ — индикатор условия $\{\cdot\}$.

Вероятность того, что выбрано сообщение M_j и при случайном выборе ключа получена криптограмма E, равна

$$P(M = M_j, E) = q_j \sum_{k=1}^{m} p_k I\{E = T_k M_j\}, \tag{3}$$

Так как $P(M = M_j) = q_j$, то условная вероятность криптограммы E при условии, что было зашифровано сообщение $M = M_j$, — это апостериорная вероятность $P_M(E)$ формально равна

$$P_M(E) = \frac{P(M, E)}{P(M)} = \sum_{k=1}^{m} p_k I\{E = T_k M\}. \tag{4}$$

Эта апостериорная вероятность зависит от сообщения M, но не зависит от априорных вероятностей $q_1, \ldots, q_n$. Формула (4) совпадает с приведенной К.Шенноном ([5, с. 362]):

> « $P_M(E)$ — условная вероятность криптограммы E при условии, что выбрано сообщение M, т. е. сумма вероятностей всех тех ключей, которые переводят сообщение M в криптограмму E. »

Известное определение условной вероятности

$$P_M(E) = \frac{P(M,E)}{P(M)}$$

не говорит о том, что при $P(M) = 0$ условной вероятности $P_M(E)$ не существует, а только о том, что в этом случае имеем неопределенность $\frac{0}{0}$, так как в этом случае и $P(M,E) = 0$. Равенство (4) вполне определяет значение условной вероятности $P_M(E)$ и в этом случае. При рассмотрении цепей Маркова, например, начинают с определения переходных вероятностей, независимо от значений начальных вероятностей. С другой стороны, так как из $P(M) = 0$ следует $P(M,E) = 0$, то по теореме Радона–Никодима ([6, с. 578]) существует производная Радона–Никодима п. н. по мере $P(M)$, которая равна условной вероятности $P_M(E)$.

Далее цитируем К. Шеннона ([5, с. 362]):

«По теореме Байеса

$$P_E(M) = \frac{P(M) \cdot P_M(E)}{P(E)}. \tag{5}$$

Для совершенной секретности системы величины $P_E(M)$ и $P(M)$ должны быть равны для всех M и E. Следовательно, должно быть выполнено одно из равенств: или $P(M) = 0$ [это решение должно быть отброшено, так как требуется, чтобы равенство осуществлялось при любых значениях $P(M)$], или же

$$P_M(E) = P(E) \text{ для любых } M \text{ и } E. \tag{6}$$

Наоборот, если $P_M(E) = P(E)$, то

$$P_E(M) = P(M), \tag{7}$$

и система совершенно секретна.»

Так К. Шеннон доказал **Теорему** ([5, Теорема 6, с. 362], [4, Theorem 9, с. 56])

> « *Необходимое и достаточное условие для совершенной секретности состоит в том, что*
>
> $$P_M(E) = P(E) \tag{8}$$
>
> *для всех M и E, т. е. $P_M(E)$ не должно зависеть от M* ».

Здесь важно то, что для каждой криптограммы E одинаковы все апостериорные вероятности $P_M(E)$, когда M принимает все значения из множества $\{M_1, \ldots, M_n\}$. Все $P_M(E)$ не зависят от априорных вероятностей $q_1, \ldots, q_n$, а их равенство априорной (безусловной) вероятности $P(E)$, вообще говоря зависящей от априорных вероятностей $q_1, \ldots, q_n$, — это следствие формулы полной вероятности.

В ходе рассуждений о теореме Байеса (5) можно было взять произвольное невырожденное априорное распределение, например, $P(M = M_j) = 1/n, j = 1, \ldots, n$, и из формулы (5) с помощью равенств $P_E(M) = P(M)$ получить требуемые равенства (6) без оговорок о $P(M) = 0$. По-видимому, К. Шеннон хотел так поступить — в квадратные скобки берется редактором текст, который предполагается удалить. А так как все величины в (6) не зависят от значений $P(M)$, то из теоремы Байеса (5) и равенств (6) следуют равенства (7) для всех M и E уже при любых значениях априорных вероятностей $P(M)$.

Вырожденные распределения вероятностей не нарушают равенства (7):

Если $P(M) = 0$, то $P(M, E) = 0$, откуда $P_E(M) = \frac{P(M,E)}{P(E)} = 0 = P(M)$;

если $P(M) = 1$, то $P(M, E) = P(E)$, откуда $P_E(M) = 1 = P(M)$, и условия (7) выполнены.

Эта теорема утверждает эквивалентность условия (7) определения совершенной секретности равенствам (6), но сформулирована без уточнения о любых значениях $P(M)$.

Не зависящие от значений $q_1, \ldots, q_n$ величины в правой части (4) $P_M(E)$ называют *переходными вероятностями шифра*. Если для криптограммы все переходные вероятности одинаковы для всех сообщений, то это говорит о том, что для этой криптограммы ни одно сообщение не имеет преимущества перед другими. Если это справедливо для любой криптограммы, то по теореме Шеннона это означает совершенную секретность.

Конкретный пример совершенно секретного шифра состоит в том, что число сообщений точно равно числу ключей и числу криптограмм ([5, с. 363]):.

> «Пусть M_i занумерованы числами от 1 до n, так же как и E_i, и пусть используются n ключей. Тогда
>
> $$T_i M_j = E_s,$$
>
> где $s = i + j (\mathrm{mod}\ n)$. В этом случае оказывается справедливым равенство $P_E(M) = \frac{1}{n} = P(E)$ и система является совершенно секретной.»

Здесь отсутствует указание на равновероятность ключей и в последней формуле $P_E(M) = \frac{1}{n} = P(E)$ очевидна опечатка. Должно быть $P_M(E) = \frac{1}{n} = P(E)$. Та же опечатка в [4, p. 56] и последующих переводах. Указание на равновероятность ключей следует позже ([5, p. 363]):

> «Совершенно секретные системы, в которых число криптограмм равно числу сообщений, а также числу ключей, характеризуются следующими двумя свойствами: 1) каждое M связывается с каждым E только одной линией; 2) все ключи равновероятны. Таким образом, матричное представление такой системы является «латинским квадратом»».

В. А. Котельников в [3] вместо термина криптограмма использует тождественный термин *сигнал*.

Сообщение — это то, что необходимо передать из одного пункта в другой. Это может быть отдельная буква, слово, депеша или даже совокупность депеш.

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

Шифром называет закон, связывающий сигналы с соответствующими сообщениями.

> «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*.»

После нестойких зашифровок 3-го и 2-го классов В. А. Котельников рассматривает:

> *«Зашифровка 1 класса* («совершенная»): 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 этом все возможные шифры известны лицу, расшифровывающему перехваченные сообщения.»

Анализируя таблицу, связывающую сообщения, шифры и получаемые сигналы (криптограммы), В. А. Котельников доказывает следующие утверждения (Положения 1 и 2 относятся к случаям нарушения секретности):

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

Учитывая то, что «каждый сигнал в любом шифре должен соответствовать одному только сообщению,(иначе–авт.) даже зная шифр, нельзя будет однозначно расшифровать сигнал», то в [3] видим шифр с «латинским квадратом» и одноразовым ключом. Вместо различных априорных вероятностей В.А.Котельников рассматривает равновероятные на различных подмножествах

множества возможных сообщений, предполагая, что «известно, что часть сообщений не передавалась».

Анализируя таблицу шифра, в качестве определения совершенной секретности В. А. Котельников рассматривает равноправность всех сообщений, как результата расшифрования любой данной криптограммы, т. е. равенство переходных вероятностей — это то, что К. Шеннон доказывает в своей теореме. Обратное утверждение о равенстве апостериорных вероятностей сообщений априорным из такого определения очевидна по формуле полной вероятности.

В отличие от К. Шеннона, В. А. Котельников применил комбинаторный подход и в 1941 году обосновал теоретическую стойкость шифра гаммирования при одноразовом использовании случайной и равновероятнойгаммы ([9]). Кроме того уже до 1945 года под его руководством были созданы средства стойкого шифрования текстовой и, что особенно сложно, речевой информации ([10]).

Автор выражает благодарность Андрею Михайловичу Зубкову за обсуждения и ценные советы.

СПИСОК ЛИТЕРАТУРЫ

1. *Андреев Н. Н.*, *Петерсон А. П.*, *Прянишников К. В.*, *Старовойтов А. В.* Основоположник отечественной засекреченной телефонной связи. — Радиотехника, 1998, в. 8, с. 8–12. // *Andreev N. N.*, *Peterson A. P.* , *Praynishnikov K. V.* , *Starovoitov A. V.* The founder of domestic secret telecommunication. — Radiotehnika, 1998, в. 8, с. 8–12. (In Russian.)
2. Биография Клода Эльвуда Шеннона. — Обозрение прикл. и промышл. матем. — 1997, т. 4, в. 2, с. 276–282. // Biography of Claud Elwood Shannon. — OP&PM Surveys Appl. Industr. Math., 1997, v. 4, is. 2, p. 276–282.
3. *Котельников В. А.* Основные положения автоматической шифровки. 19 июня, 1941. В сб.: Котельников В. А. Собрание трудов. Том 1. Радиофизика, информатика, телекоммуникации. // *Kotel'nikov V. A.* Substantive provisions of an automatic encryption. On June, 19, 1941. In Book: Kotel'nikov V. A. Assembly of works. V. 1. Radiophysics, computer science, telecommunications. (In Russian.)
4. *Shannon C. E.* A Mathematical Theory of Cryptography. September 1, 1945,132 p.
5. *Шеннон К.* Теория связи в секретных системах.— Пер. с англ. В. Ф. Писаренко, с. 333—402. В кн.: Работы по теории информации и кибернетике. Перевод с англ. под ред. Р. Л. Добрушина и О. Б. Лупанова. М., ИЛ, 1963, 830 с. // *Shannon C. E.* Communication Theory of Secrecy Systems. — Bell System Technical Journal, 1949, v. 28, n. 4, p. 656–715.
6. *Боровков А. А.* Теория вероятностей: Учебное пособие. Изд. 5-е, сущ. перераб. и доп. М.: Книжный дом «ЛИБРОКОМ», 2009, 656 с. // *Borovkov A. A.* Probability theory: The manual. Edition 5-th. M.: The Book house “LIBROKOM”, 2009, 656 p. (In Russian.)
7. *Алферов А. П.*, *Зубов А. Ю.*, *Кузьмин А. С.*, *Черемушкин А. В.* Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. М.: Гелиос АРВ, 2005, 480 с., ил. // *Alferov A. P.*, *Zubov A. Y.*, *Kuzmin A. S.*, *Cheremushkin A. V.* Bases of cryptography: The manual. 3-th edition. M.: Gelios ARV, 2005, 480 p. (In Russian.)
8. *Зубов А. Ю.* Совершенные шифры. — М.: Гелиос АРВ, 2003, 160 с. // *Zubov A. Y.* The perfect secrecy systems. — M.: Gelios ARV, 2003, 160 p. (In Russian.)
9. *Сачков В. Н.* Становление и развитие современной отечественной криптографии. — Математические вопросы криптографии. 2022, т. 13, в. 2, с. 7–15. // *Sachkov V. N.* Becoming and development of modern domestic cryptography. — Math. Asp. Cryptogr., 2022, v. 13, is. 2, p. 7–15. (In Russian.)

10. *Бутырский Л. С.*, *Ларин Д. А.*, *Шанкин Г. П.* Криптографический фронт Великой Отечественной. М.: Гелиос АРВ, 2017,688 с., ил.// *Butyrskiy L. S.*, *Larin D. A.*, *Shankin G. P.* Cryptographic front Great Patriotic War. M.: Gelios ARV, 2017, 688 p. (In Russian.)

Поступила в редакцию
23.VI.2024

UDC 519.719.2 DOI https://doi.org/10.52513/08698325_2024_31_1_1

Serov S. I. (Moscow, Review of applied and industrial mathematics)**. The role of a priori probabilities in a perfect secrecy's question of Kotel'nikov–Shannon.**

Abstract: The perfect secrecy of the system does not depend on values of a priori probabilities of messages.

Keywords: cipher, perfect secrecy, a priori probabilities