Философский журнал
2016. Т. 9. № 3. С. 148–153
УДК 165.64

The Philosophy Journal
2016, vol. 9, no 3, pp. 148–153
DOI 10.21146/2072-0726-2016-9-3-148-153

А.А. Парамонов

КОГДА ТАЙНОЕ ОСТАЕТСЯ ТАЙНЫМ*

Парамонов Андрей Альбертович – кандидат философских наук, научный сотрудник сектора аналитической антропологии. Институт философии РАН. Российская Федерация, 109240, г. Москва, ул. Гончарная, д. 12, стр. 1; доцент Школы философии. Высшая школа экономики. Российская Федерация, 101000, г. Москва, ул. Мясницкая, д. 20; e-mail: andrei-paramonov@yandex.ru

Рассматривается фрагмент из книги Фрэнсиса Бэкона «О достоинстве и приумножении наук» (“De Dignitate et Augmentis Scientiarum”, 1623), в котором английский философ объясняет придуманный им прием сокрытия тайного текста с использованием двух шифровальных алфавитов. Стратегией сокрытия у Бэкона может выступать не только принцип незаметности присутствия в письме тайного содержания, которому, например, следует его знаменитый метод двухлитерного шифра, но и прямо противоположный, когда средством утаивании выступает явность тайного. Именно последний принцип и лежит в основе приема сокрытия шифра с использованием двух алфавитов. К сожалению, русский перевод фрагмента с изложением этого метода, предлагаемый в академическом издании трудов Фрэнсиса Бэкона (1977), приводит к ошибкам в понимании изобретения Бэкона. В статье дан комментарий к существующему переводу этого фрагмента и предложен другой вариант перевода.

Ключевые слова: Фрэнсис Бэкон, шифр, двухлитерный шифр, алфавит, прием сокрытия текста, использующий два шифровальных алфавита

…Мелькают смыслы, замечанья,
Портреты, числа, имена,
Да буквы, тайны письмена…

А.С. Пушкин

Понимание не всегда приходит сразу во время чтения. Порой к пониманию прочитанного приводит незначительное замечание, брошенное где-то в отношении этого текста другим автором, замечание на первый взгляд почти случайное и, быть может, даже неточное, но привлекшее почему-то внимание и побудившее вновь вернуться к источнику.

Таким поводом обратиться к Бэкону стало для меня замечание, которое делает автор статьи «К двухлитерному шифру Фрэнсиса Бэкона», приводя цитату из книги «О достоинстве и приумножении наук», речь в которой идет об использовании двух алфавитов для сокрытия секретного послания. Автор статьи относит, и как мне кажется теперь, ошибочно, цитируемый фрагмент к предварительному описанию двухлитерного шифра, подробное изложение

* Статья представляет собой отклик на публикацию: *Ефишов И.И.* К двухитерному шифру Фрэнсиса Бэкона. С. 135–147 наст. изд.

которого Бэкон действительно начинает в следующем за этим фрагментом абзаце. По крайней мере такое толкование следует из предложения автора понимать под двумя алфавитами, о которых там говорится, два разных типа начертания букв. Именно это замечание, а также избирательное цитирование в упомянутой статье данного фрагмента и привлекли вновь мое внимание в изначальному тексту Бэкона о шифрах.

Известно, что Фрэнсис Бэкон был знаком с криптографией не понаслышке, он начинал свою карьеру со службы в английском посольстве при французском дворе, где выполнял дипломатические поручения. Именно в Париже ему, по собственному признанию, пришла идея двухлитерного шифра. Основы представлений о шифрах и свои открытия в этой области впервые подробно изложил в книге «О достоинстве и приумножении наук», которая вышла в 1623 г.[1].

Знание тонкостей шифровального искусства, слава первооткрывателя принципа бинарного кодирования – с одной стороны, с другой – богатая палитра языка и блестящий стиль изложения, вкупе с образом царедворца, чья жизнь рисуется полной тайн и интриг, породили непреходящий миф о существовании секретных записей в произведениях Бэкона, а почитатели его таланта до сих пор ищут зашифрованные свидетельства авторства Бэкона в творениях Шекспира. Возможно, именно этим объясняется стремление редакторов некоторых латинских изданий «О достоинстве и приумножении наук» сохранять явно ошибочные вставки, появившиеся в одном первых переизданий книги в изначально правильном тексте. И что удивительно, эти вставки оказались именно на тех страницах книги, где Бэкон раскрывает принципы двухлитерного шифра[2].

Мартин Гарднер, американский математик, известный популяризатор науки, автор книги о шифрах[3], приписывает Бэкону помимо изобретения двухлитерного шифра еще одно изобретение в области криптографии. Он пишет: «Бэкон был первым, кто изложил хитроумный прием сокрытия текста, использующий два шифровальных алфавита»[4]. В отличие от двухлитерного шифра, этот метод шифрования Бэкона почти неизвестен.

Фрагмент из книги «О достоинстве и приумножении наук», в котором, как можно предположить, излагается этот метод, звучит в современном академическом переводе следующим образом:

> Нужно иметь два алфавита: один – состоящий из обычных букв, другой – из букв, не имеющих никакого значения, и отправить одно в другом сразу два письма: одно – содержащее секретные сведения, другое – имеющее достаточно правдоподобное для пишущего содержание, которое, однако, не должно навлечь на него никакой опасности. И если вдруг начнут строго допрашивать о шифре, то нужно дать алфавит, состоящий из ничего не значащих букв, вместо алфавита из настоящих букв и алфавит, состоящий из настоящих букв, вместо алфавита из букв, не имеющих значения. Таким образом, следователь сможет прочитать внешнее письмо и, найдя его вполне правдоподобным, ничего не заподозрит о существовании внутреннего письма[5].

---

1 См.: *Bacon F.* Opera. T. I: Qui continet «De dignitate et augmentis scientiarum» libros IX. Londini, 1623. P. 277–283.

2 См.: *Bacon F.* De Augmentis Scientiarum. Lib. IX. Amstelædami, 1662. P. 351–352; *Idem*. De Dignitate et Augmentis Scientiarum. T. II. Wirceburgi, 1780. P. 78–79; *Idem*. De Dignitate et Augmentis Scientiarum. Libri IX: Ad fidem optimarum editionum edidit vitamque auctiris adjecit Phillippus Mayer. T. II. Norinbergae, 1829. P. 60–61.

3 *Gardner M.* Codes, Ciphers and Secret Writing. N.Y., 1972.

4 *Гарднер М.* Шифр Бэкона // Квант. 1992. № 8. С. 21.

5 *Бэкон Ф.* Соч.: 2 т. Т. 1. 2-е изд. М., 1977. С. 338.

Вряд ли на основании приведенного перевода кто-то сегодня может объяснить, в чем же действительно состоит предлагаемый Бэконом метод сокрытия секретного сообщения. Именно к этому фрагменту и относится упомянутое выше замечание в статье И.И. Ефишова. Возможно, что своим замечанием и тем, что в качестве цитаты были выбраны лишь первые и последние строки фрагмента, автор статьи невольно попытался придать хоть какой-то смысл этому странному описанию. Но даже если не вдаваться в логику предлагаемых действий по сокрытию секрета в перехваченном письме, сомнения возникают относительно самой возможности существования «букв, не имеющих значения» и алфавита из этих «букв». Более того, как будет показано, именно очевидная невозможность их существования и позволяет допрашиваемому утаить секретное послание.

В чем же в действительности состоит метод шифрования, о котором идет речь в этом фрагменте, и в чем причина трудностей его понимания?

В своей книге «О достоинстве и приумножении наук» изложение этого метода Бэкон предваряет перечислением известных ему типов шифров, останавливаясь также на качествах, которыми должны обладать лучшие из них. Одно из таких качеств, выделяемых им, можно определить как скрытость шифра, незаметность его присутствия в тексте. Шифры, пишет Бэкон, «не должны вызывать подозрения»[6]. Именно таким качеством, по его мнению, обладает разработанный им двухлитерный шифр, наличие которого в написанном ничем не примечательным почерком письме любого содержания обнаружить чрезвычайно трудно.

Но оказывается, что добиться неприметности шифра можно, прибегнув и к прямо противоположной стратегии, когда письмо с секретным содержанием всем своим видом показывает, что оно несет зашифрованное сообщение, например когда оно представляет собой последовательность непонятных непосвященному знаков. Можно сказать, что именно в утаивании присутствия в тексте тайного шифра с помощью нарочито секретного вида письма и состоит предлагаемый Бэконом метод шифрования с помощью двух алфавитов.

Следуя Гарднеру, этот метод можно описать следующим образом. Для начала составляются два шифрованных набора знаков или букв, их Бэкон для краткости называет алфавитами[7]. Буквами одного алфавита записывается секретное сообщение, буквами другого – сообщение несекретного характера. Затем оба сообщения вкладываются одно в другое так, что буквы одного перемежаются буквами другого. Получившееся в результате этого послание может быть отправлено адресату, которому заранее известны оба алфавита. В случае если письмо будет перехвачено, а отправитель или адресат принуждены к ответу, то допрашиваемому следует выдать в качестве секретного алфавита тот набор знаков, которым на самом деле написано несекретное письмо. Знаки же, которыми написано настоящее секретное письмо, нужно объявить незначащими, т. е. такими, которые были введены в текст якобы лишь с целью создания дополнительных препятствий расшифровке письма. Естественно, что такого рода пустые знаки не предполагают за собой ни алфавита, ни шифра. В результате требования допрашивающей стороны оказываются удовлетворены: предоставлен шифр, с помощью которого зашифрованное сообщение может быть прочитано. Но и подозреваемый не ском-

---

6 *Бэкон Ф.* Указ. соч. С. 337.

7 Говоря о возможности передачи сообщений с помощью письма, Бэкон замечает, что последнее «осуществляется либо с помощью обычного алфавита, принятого повсеместно, либо с помощью особого, тайного алфавита, известного лишь немногим; такой алфавит называется шифром» (Там же).

прометирован содержанием этого сообщения. При этом шифр настоящего секретного послания, как и оно само, остаются нераскрытыми, поскольку их существование при таком развитий событий даже и не предполагается. Бэкон не математик, он – царедворец, знающий тонкости человеческой натуры.

В чем же состоит трудность перевода фрагмента, в котором Бэкон излагает этот метод? Одно из обстоятельств заключается в исключительной краткости описания – всего несколько строк. В оригинальном тексте прижизненного издания 1623 г. этот фрагмент выглядит так:

> Hoc hujusmodi est: Vt hobeat quis duo Alphabeta: Vnum Literarum verarum, alterum Non-significantium; Et simul duas Epistolas inuoluat: vnam, quae secretum deferat, alteram, qualem verisimile fuerit Scribentem missurum fuisse, absque periculo tamen. Quod si quis de Ciphra seuere interrogetur, porrigat ille Alphabetum Non-significantium, pro veris Literis, Alphabetum autem Verarum Literarum pro Non-significantibus; hoc modo incidet Examinator in Epistolam illam Exteriorem, quam cum probabilem inueniet, de Interiori Epistola nihil suspicabitur[8].

Другое обстоятельство, на мой взгляд, состоит в использовании Бэконом всей смысловой палитры слова *litera* (в современном написании *littera*). Так, на предшествующих фрагменту страницах, где Бэкон рассуждает о грамматике, это слово в зависимости от контекста может прочитываться не только как «буква» или «буквы», но также и как «дисциплина» или «письменность». В случае же интересующего нас фрагмента интервал изменения контекста, определяющего значение слова *litera,* не выходит даже за рамки одного предложения. Заметим, что здесь слово *litera* стоит только во множественном числе. И если воспользоваться такими однокоренными в русском языке эквивалентами *leterae*, как «письмо» и «письмена», то можно предложить следующий вариант перевода фрагмента:

> Это средство сводится к следующему. Нужно иметь два алфавита: один – для истинного письма [Literarum verarum], другой – для незначимого [Non-significantium], и вложить вместе одно в другое два послания: одно – содержащее секретные сведения, другое будет написано как правдоподобное, которое может быть отправлено, однако, без какого-либо опасения. Так что если кого-то начнут строго спрашивать о шифре, то следует представить тот алфавит для незначимого письма [Alphabetum non significantium] как истинные письмена [pro veris Literis], алфавит же для истинного письма [Alphabetum autem Verarum Literarum] – как незначимые [pro Non-significantibus]. В результате следователь овладеет тем внешним посланием и, найдя его вполне правдоподобным, не заподозрит внутреннего послания.

В заключение приведу для сравнения два перевода этого фрагмента на английский.

Один из этих переводов из издания 1853 г., близок к русскому академическому переводу:

> There is a new and useful invention to elude the examination of a cipher; viz., to have two alphabets, the one of significant, and the other of non-significant letters; and folding up two writings together, the one conveying the secret, whilst the other is such as the writer might probably sond without danger. In case of a strict examination about the cipher, the bearer is to produce the non-significant alphabet for the true, and the true for the non-significant; by which means the examiner would fall upon the outward writing, and finding it probable, suspect nothing of the inner[9].

---

8 *Bacon F.* Opera. T. I: Qui continet «De dignitate et augmentis scientiarum» libros IX. P. 278.

9 *Bacon F.* The Physical and Metaphysical Works. L., 1853. P. 222.

Стоит отметить, что редактор этого издания книги и ее переводчик Джозеф Денви (Joseph Denvey) в своем примечании высказывает некоторые сомнения в эффективности предложенного Бэконом метода, которые в определенной мере можно объяснить неточной интерпретацией последнего: «Обнародование этого секрета сводит на нет его интенцию, поскольку проверяющий, хотя он и найдет внешнее письмо правдоподобным, останется в сомнениях, когда, будучи таким образом уведомленным, проверит внутреннее письмо, несмотря на то, что его алфавит будет выдан ему как незначащий»[10].

Интересное решение найдено в издании 1861 г. под редакцией Джеймса Спеддинга (James Spedding), в котором перевод оставляет окончательную интерпретацию текста за читателем, и решающую роль в этом будет играть выбор смысла слова *letter*:

> It is this: let a man have true alphabets, one of true letters, the other of non-significants; and let him infold in them two letters at once; one carrying the secret, the other such a letter as the writer would have been likely to send and yet without anything dangerous. Then if any one be strictly examined as to the cipher, let him offer the alphabet of non-significants for the true letters and the alphabet of true letters for non-significants. Thus the examiner will fall upon the exterior letter; which finding probable, he will not suspect anything of another letter within[11].

Конечно, можно отчасти согласиться с Джозефом Дэнви: обнародование любого метода сокрытия тайного не способствует его последующему успешному применению. Однако процесс обнародования может затянуться на годы.

Автор приносит благодарность Светлане Сергеевне Неретиной за уроки латыни.

Список литературы

Бэкон Ф. Соч.: 2 т. Т. 1. 2-е изд., испр. и доп. / Под ред. А.Л. Субботина. М.: Мысль, 1977. 567 с.

Гарднер М. Шифр Бэкона / Пер. с англ. Ю. Данилова // Квант. 1992. № 8. С. 21–26.

Bacon F. Opera. T. I: Qui continet “De dignitate et augmentis scientiarum” libros IX. Londini: In Officina Ioannis Haviland, 1623.

Bacon F. De Augmentis Scientiarum. Lib. IX. Amstelædami: Sumptibus Joanmis Ravelteinÿ, 1662.

Bacon F. De Dignitate et Augmentis Scientiarum. T. II. Wirceburgi: Apud Jo. Jac. Stahel, 1780.

Bacon F. De Dignitate et Augmentis Scientiarum. Libri IX: Ad fidem optimarum editionum edidit vitamque auctiris adjecit Phillippus Mayer. T. II. Norinbergae: Sumptibus Rigelii et Wiefsneri, 1829.

Bacon F. The Physical and Metaphysical Works / Ed. by J. Devey. L.: Hery G. Bohn, 1853.

Bacon F. The Philosophical Works. Vol. IV / Ed. by J. Spedding. L.: Taggard & Thompson, 1861.

Gardner M. Codes, Ciphers and Secret Writing. N.Y.: Simon and Schuster, 1972. 96 p.

[10] *Bacon F.* The Physical and Metaphysical Works. P. 222n.

[11] *Bacon F.* The Philosophical Works. Vol. IV. L., 1861. P. 445.

When the hidden remains hidden

Andrei Paramonov

PhD, Research Fellow. Institute of Philosophy, Russian Academy of Sciences. 12/1 Goncharnaya Str., Moscow, 109240, Russian Federation; Associate Professor, School of Philosophy. National Research University Higher School of Economics. 20 Myasnitskaya Str., Moscow, 101978, Russian Federation; e-mail: andrei-paramonov@yandex.ru

In the present article, Andrei Paramonov brings under a close examination the fragment of Francis Bacon's 1623 book De Augmentis Scientiarum (*On the Advancement of Learning*) where the philosopher explains his invention of the method of hiding a secret message by means of two specially devised cipher alphabets. It is argued that along with the principle of imperceptibility of the hidden message present in writing, a good illustration of which gives his famous method of biliteral cipher (an analysis of which one finds in Ivan Efishov's paper published in this volume), Bacon also adopts the opposite strategy where the very apparency of the hidden is the instrument of concealment. It is the latter principle that underlies the method of hiding the secret message by using the two alphabets. Unfortunately, the existing Russian translation of the chapter expounding this method, which is contained in two-volume academic edition of Bacon's works published in 1977, is so imprecise that no adequate understanding of Bacon's invention can be derived from it. Dr. Paramonov discusses the existing text and suggests a corrected translation of the relevant passages.

Keywords: Francis Bacon, cipher, biliteral cipher, method of steganography using two cipher alphabets

References

Bacon, F. *Opera*, T. I: Qui continet *De dignitate et augmentis scientiarum* libros IX. Londini: In Officina Ioannis Haviland, 1623.

Bacon, F. *De Augmentis Scientiarum*, Lib. IX. Amstelædami: Sumptibus Joanmis Ravelteinÿ, 1662.

Bacon, F. *De Dignitate et Augmentis Scientiarum*, T. II. Wirceburgi: Apud Jo. Jac. Stahel, 1780.

Bacon, F. *De Dignitate et Augmentis Scientiarum*, Libri IX: Ad fidem optimarum editionum edidit vitamque auctiris adjecit Phillippus Mayer. T. II. Norinbergae: Sumptibus Rigelii et Wiefsneri, 1829.

Bacon, F. *The Physical and Metaphysical Works*, ed. by J. Devey. London: Hery G. Bohn, 1853.

Bacon, F. *The Philosophical Works*, Vol. IV, ed. by J. Spedding. London: Taggard & Thompson, 1861.

Bacon, F. *Sochineniya* [Selected Works], Vol. 1, ed. by A. Subbotin, 2nd ed. Moscow: Mysl' Publ., 1977. 567 pp. (In Russian)

Gardner, M. "Shifr Bekona" [Bacon's Cipher], trans. by Yu. Danilov, *Kvant*, 1992, No. 8, pp. 21–26. (In Russian)

Gardner, M. *Codes, Ciphers and Secret Writing*. New York: Simon and Schuster, 1972. 96 p.