Философский журнал
2016. Т. 9. № 3. С. 135–147
УДК 165.64

The Philosophy Journal
2016, vol. 9, no 3, pp. 135–147
DOI 10.21146/2072-0726-2016-9-3-135-147

ДИСКУССИИ

И.И. Ефишов

К ДВУХЛИТЕРНОМУ ШИФРУ ФРЭНСИСА БЭКОНА

Ефишов Иван Иванович – кандидат физико-математических наук, доцент кафедры компьютерной безопасности. Балтийский федеральный университет имени И. Канта. Российская Федерация, 236016, г. Калининград, ул. А. Невского, д. 14; старший научный сотрудник. Калининградский филиал Института земного магнетизма, ионосферы и распространения радиоволн имени Н.В. Пушкова РАН. Российская Федерация, 236010, г. Калининград, пр-т Победы, д. 41; e-mail: IEfishov@kantiana.ru

Во втором, исправленном и дополненном издании сочинений Ф. Бэкона, выпущенном в 1977 г., в главе I книги VI трактата «О достоинстве и приумножении наук» были сделаны досадные ошибки криптографического характера. Все они касаются двухлитерного (двухбуквенного) шифра, разработанного самим ученым, по его словам, еще в юности. Эти ошибки (различного происхождения) частично искажают мысли английского философа, основоположника эмпиризма и государственного деятеля, о «высшей ступени совершенства шифра», ныне называемого также шифром (или кодом) Бэкона. Кроме того, они обесценивают примеры, тщательно подобранные и приведенные ученым в трактате. Интересно отметить, что в первом прижизненном издании вышеупомянутого трактата на латинском языке (1623) подобных ошибок не было. Из чего мы можем сделать вывод, что Бэкон более внимательно относился к изданию своих трудов, нежели философская редакция издательства, выпустившая его труды через триста пятьдесят лет. Последовательность из символов 0 и 1 (или, если угодно, из «двух букв» a и b, как в сочинении Бэкона) является двоичной последовательностью, без которой теперь немыслима работа ни одного компьютера. Ученый словно предчувствовал большое будущее у такого способа передачи информации: «…это изобретение приводит нас к чрезвычайно важным выводам. Ведь из него вытекает способ, благодаря которому с помощью любых объектов, доступных зрению или слуху, мы можем выражать и передавать на любое расстояние наши мысли». Увы, от ошибок, искажающих мысли, не застрахован никто. В статье проанализированы эти ошибки (и опечатки), а также даны рекомендации по внесению необходимых исправлений в соответствующую главу труда «О достоинстве и преумножении наук».

Ключевые слова: Бэкон, двухлитерный шифр, шифр, двоичный код

Omnia per omnia

Фрэнсис Бэкон (1561–1626) «еще в ранней юности», когда ему было всего семнадцать лет, изобрел шифр, который, как он сам пишет, «представляет собой высшую ступень совершенства шифра, давая возможность выражать все через все (omnia per omnia)»[1]. В это время (1576–1579) Бэкон служил в составе английской миссии в Париже, где, вероятнее всего, впервые и познакомился (или, во всяком случае, имел дело) с дипломатическими шифрами. В 1579 г. он вернулся в Англию. Однако первое краткое упоминание о своем шифре ученый привел только через двадцать семь лет в работе «О преумножении наук» (1605). Более подробно двухлитерный шифр описан в трактате «О достоинстве и приумножении наук» (1623), книга VI, глава I.

Интересно отметить, что в 1586 г. французский ученый Блез де Виженер также в Париже издает свой трактат “Traicté des Chiffres ou Secrètes Manières d’Escrire” («Трактат о Цифрах и Тайнописи»). Нет никаких оснований подвергать сомнению слова Бэкона о том, что он изобрел свой шифр ранее 1586 г., тем не менее француз опередил англичанина с публикацией, в которой описал тот же самый шифр. Хотя, возможно, оба они заимствовали этот шифр у более ранних криптологов, например у итальянца Джамбаттисты делла Порты (1535–1615)[2]. Идеи и впрямь витают в воздухе!

Несомненно, что именно Ф. Бэкон был первым среди вышеназванных персон, кто обратил внимание на наиболее существенное обстоятельство: «…это изобретение приводит нас к чрезвычайно важным выводам. Ведь из него вытекает способ, благодаря которому с помощью любых объектов, доступных зрению или слуху, мы можем выражать и передавать на любое расстояние наши мысли, если только эти объекты способны выражать хотя бы два различия. Такими средствами могут быть: звук колоколов или рога, пламя, звуки пушечных выстрелов и т. п.»[3]. Со временем человечество усовершенствует способы передачи информации: телеграф, радио, Интернет… А пока что хватало звона колокола…

Основные принципы двухлитерного шрифта

В рассматриваемой нами части трактата Фрэнсис Бэкон рассказывает об искусстве шифрования в следующих словах: «Существует довольно много видов шифра: простые шифры, шифры, смешанные со знаками, ничего не обозначающими, шифры, изображающие по две буквы в одном знаке, шифры круговые, шифры с ключом, шифры словесные и т. д. Шифры должны обладать тремя достоинствами: они должны быть удобными, не требующими многих усилий для их написания; они должны быть надежны и ни в коем случае не быть доступны дешифровке и, наконец, если это возможно, они не должны вызывать подозрения. Ведь если письма попадут в руки тех, кто обладает властью над тем, кто пишет это письмо, или над тем, кому оно адресовано, то, несмотря на надежность шифра и невозможность его прочесть, может начаться расследование соответствующего дела, если только шифр не будет таким, что не вызовет никакого подозрения или же ничего не даст при его исследовании»[4].

---

1 *Бэкон Ф.* Соч.: 2 т. Т. 1. 2-е изд. М., 1977. С. 323.

2 *Pesic P.* The clue to the labyrinth: Francis Bacon and the decryption of nature // Cryptologia. 2000. Vol. XXIV. № 3. P. 200.

3 *Бэкон Ф.* Указ. соч. С. 323.

4 Там же. С. 322.

Обратим особое внимание на третье условие: шифры «не должны вызывать подозрения». Это редкое требование к шифрам; Бэкон думает не только о самом процессе шифрования, но также и о сокрытии факта существования секретного сообщения в «невинном» на первый взгляд послании. Ведь если, перехватив письмо, вы заметите в нем некий бессмысленный текст, например «ffff uuu gg e», то вы вправе заподозрить, что здесь применен некий шифр.

Как высший сановник Великобритании, лорд-хранитель печати (с 1617 г.), а затем лорд-канцлер (1618–1621) ученый вынужден был думать о надежных способах сохранения тайны дипломатической корреспонденции: «…учение о дешифровке… это, конечно, очень трудное дело, требующее в то же время большой изобретательности; это искусство (точно так же, как и искусство шифра) используется в секретных государственных делах»[5]. Бэкон нашел выход в шифре собственного изобретения, посредством которого сообщение не только шифруется, но и прячется в самом обычном тексте, «маскируется» под него. Бэкон приводит следующий пример такой маскировки: “Ma**n**e**re** te **v**o**l**o **do**nec **v**enero” («Я хочу, чтобы ты оставался на месте, пока я не приду»)[6]. Как видим, в этой фразе нет ничего необычного. Но здесь Бэконом намеренно выделены **полужирным** начертанием (то есть фактически вторым шрифтом) некоторые буквы: **n, r, e, v, o, d, o** и **v.** Ученый советует подбирать шрифты едва отличимыми друг от друга. То есть такими, что только заранее осведомленный человек, знающий о различии шрифтов, смог бы понять их разницу. Здесь реализован принцип стеганографии[7]: даже перехватив само послание, вы ничего странного в нем не заметите, даже не будете подозревать, что здесь что-то не так.

Как видим, все дело в двух различных шрифтах. Вот что пишет по этому поводу сам Бэкон: «Нужно иметь два алфавита[8]: 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»[9]. Таким образом, можно «прочитать внешнее письмо и, найдя его вполне правдоподобным, ничего не заподозрить о существовании внутреннего письма»[10].

Для дешифровки необходимо применить следующий алгоритм. На первом шаге разобьем исходный текст на составные части из пяти букв следующим образом:

Ma**n**e**r** || **e** te **vo** || lo **do**n || ec **v**en || [ero].
(Я хоч**у**, || чт**об**ы || ты о**ст** || а**в**ал**с** || [я на месте, пока я не приду]).

Лишь теперь, после разбиения фразы на пятерки букв, мы видим, что дешифруемое слово состоит ровно из четырех букв. Выделенные буквы в пятерках оригинала и перевода не совпадают по местам, так как дешифруемое слово в русском переводе не является калькой с латинского и поэтому

---

5 *Бэкон Ф.* Указ. соч. С. 325.

6 Там же. С. 324.

7 Термин происходит от двух греч. слов *στεγανός* – скрытый и *γράφω* – пишу; буквально «тайнопись». Стеганография скрывает наличие секретного сообщения, которое может быть написано просто обычным письмом. Данный метод противоположен шифрованию. Шифры не скрывают наличия секретного сообщения, они лишь делают его нечитабельным для посторонних лиц.

8 Под алфавитом в данном контексте Ф. Бэкон имеет в виду шрифт.

9 Там же. С. 322.

10 Там же. С. 323.

пишется иначе. В квадратных скобках заключен лишний текст, который не использовался при шифровании; при дешифровке он легко будет отброшен как ненужный.

На втором шаге необходимо перевести полученную информацию в *двоичный код*. Для этого буквы обычного шрифта (*первого алфавита*) заменяем буквой a, буквы с **полужирным** начертанием шрифта (это *второй алфавит*, состоящий из других литер, отличных начертанием от «первых») – b. Получим:

aabab || *baabb* || *aabba* || *aabaa*.
(*aaaab* || *aabab* || *aaabb* || *abbab*).

На последнем, третьем, шаге алгоритма остается только свериться с алфавитом самого шифра (см. табл. 1). Прописными буквами в нем обозначен обычный латинский алфавит (состоящий из 24 букв). Двухлитерный алфавит здесь является шифралфавитом, который записан выше строчными *курсивными* буквами.

Таблица 1

Открытый (латинский) алфавит и соответствующий ему двухлитерный шифралфавит

A	B	C	D	E	F
aaaaa	*aaaab*	*aaaba*	*aaabb*	*aabaa*	*aabab*
G	H	I	K	L	M
aabba	*aabbb*	*abaaa*	*abaab*	*ababa*	*ababb*
N	O	P	Q	R	S
abbaa	*abbab*	*abbba*	*abbbb*	*baaaa*	*baaab*
T	V	W	X	Y	Z
baaba	*baabb*	*babaa*	*babab*	*babba*	*babbb*

Напомним, что в классическом латинском алфавите 23 буквы. Здесь же присутствуют 24 буквы, поскольку Бэконом также добавлена буква W (она возникает как удвоение V). В средневековой, как и в классической, латыни отсутствовала также буква U. Существовала только буква V, которая играла роль и согласной V, и гласной U.

Итак, секретное послание в вышеприведенном примере, состоящее из одного слова, – это FVGE (совр. написание fuge, *лат*. беги), т. к. F в шифралфавите соответствует *aabab*, V – *baabb*, G – *aabba*, E – *aabaa*. Хотя нами опущен русский вариант табл. 1, но и из него точно так же получилось бы при дешифровке БЕГИ (здесь и далее буквы обычного, или *открытого*, алфавита будем, как это принято в криптографии, писать ПРОПИСНЫМИ; буквы же шифралфавита, или *закрытого* алфавита, – строчными).

Бэкон пишет: «*Перестановки* из двух букв по пяти дадут нам тридцать два различных *сочетания*, что более чем достаточно для замещения двадцати четырех букв, из которых состоит наш алфавит»[11]. Так что, замещая, например, «Ъ» и «Ь» одной и той же *перестановкой*, мы зашифруем все тридцать три буквы русского алфавита. Как видим, *двухлитерный шифр* Бэкона применим не только для латинского алфавита, но и для других (в том числе русского).

[11] *Бэкон Ф.* Указ. соч. С. 323.

Интересно заметить еще одну особенность *двухлитерного шрифта*: *внешнее* маскирующее *письмо* может быть написано на одном языке, а *внутреннее* секретное *письмо* – на любом другом. Данное свойство шифра является еще одним его преимуществом.

Имел ли данный шифр недостатки? Типографское искусство в те времена «по современным меркам стояло на столь низком уровне, что при разглядывании в сильную лупу двух отпечатков одной и той же литеры на одной и той же странице всегда можно было обнаружить небольшие различия. Свинцовые литеры были несовершенны, набор нередко повреждался, типографская краска высыхала неравномерно на грубой увлажненной бумаге, к тому же наборщики часто путали два шрифта на одной и той же странице»[12]. Как видим, прежде всего у шифра были внешние объективные недостатки, вызванные несовершенством типографской техники, требуемой для его реализации.

Бэкон приводит и «более полный пример такого шифра»[13]. В этом примере *внешним письмом* является отрывок из первого письма от 13 января 56 г. до Р. Х. Марка Туллия Цицерона проконсулу Публию Корнелию Лентулу Спинтеру. Ниже он приведен в академической редакции 1977 г.[14].

«E**go** omni **o**ff**i**cio, ac po**ti**us pie**ta**te erga te, ca**e**te**r**is satis**f**a**c**io o**mn**i**bus**: m**i**hi ip**se** nunqu**am** satis**f**acio. **T**an**ta** **e**st **e**nim m**a**gni**t**udo tu**o**ru**m**, erga me **me**ri**t**or**u**m, **u**t qu**o**n**ia**m **t**u, nis**i** **p**er**f**ecta **r**e, d**e** me n**o**n **c**onqu**i**est**i**: e**g**o, qu**ia** no**n** **id**em in t**u**a ca**u**sa **eff**i**c**io, **v**it**i**um **mi**hi e**s**se a**c**e**r**bum put**e**m. I**n** caus**a** **ha**e**c** sunt: **Am**mon**i**us reg**i**s **l**egat**u**s a**p**erte **p**e**cu**ni**a** n**o**s oppu**g**nat. Res **a**gitur p**e**r eosd**e**m cre**di**tores, per **quos**, **c**um **tu** ad**e**ras, a**g**e**b**a**t**ur. Regi**s** caus**a**, **s**i **q**ui s**u**nt, **qui** ve**l**i**n**t, qui **p**au**ci** **s**unt, **o**m**n**e**s** a**d** Pompe**i**um rem **d**e**f**erri vol**u**nt. S**e**n**a**tus **r**e**l**i**g**i**o**n**is** ca**l**umn**iam**, no**n** **re**-lig**ion**e, s**ed** **m**alev**o**l**en**tia, **et** **ill**ius **r**e**g**iae **l**ar**g**it**i**on**is** in**vid**i**a**, com**prob**at, etc.»[15].

Соответствующее ему скрытое, *внутреннее письмо* – это **письмо спартанцев**, посланное ими некогда на скитале[16]: “Perditae res: Mindarus cecidit: milites esuriunt: neque hinc nos extricare, neque hic diutius manere possumus” («Все погибло. Миндар убит. Воины голодают. Мы не можем ни уйти отсюда, ни оставаться здесь дольше»)[17].

Бэкон отмечал, что «единственным условием при этом (при шифровании. – *И.Е.*) оказывается то, что *внутреннее письмо* должно быть в пять раз меньше *внешнего*; никаких других условий или ограничений не существует»[18]. Во *внутреннем письме* у нас ровно 91 буква. Отрывок из Цицерона

---

12 *Гарднер М.* Шифр Бэкона // Квант. 1992. № 8. С. 23.

13 *Бэкон Ф.* Указ. соч. С. 324.

14 Там же. С. 325.

15 Традиционный перевод: «Всем сознанием своего долга перед тобой или, лучше сказать, уважением к тебе я удовлетворяю всех прочих, но никак не удовлетворяю себя самого, ибо твои заслуги передо мной так велики – ведь ты не успокоился, пока мое дело не было завершено, – что жизнь кажется мне горькой, если я не поступаю так же в твоем деле. Положение вот какое: посол царя Аммоний открыто осаждает меня посредством денег; дело ведется через тех же заимодавцев, через которых оно велось, когда ты был здесь; если и находятся люди, настроенные в пользу царя, – их немного, – то все же все хотят, чтобы дело было поручено Помпею; сенат одобряет прием религиозного запрета не из соображений религии, а по недоброжелательности и из зависти к известной щедрости царя» (*Цицерон.* Письмо. XCIV. 1).

16 Скитала (от *греч.* σκυτάλη, жезл) – шифр, известный также и как шифр Древней Спарты, представляет собой устройство, используемое для осуществления шифрования; оно состоит из цилиндра (жезла) и узкой полоски пергамента (обматывавшейся вокруг него по спирали), на которой писалось сообщение вдоль длины цилиндра. Когда полоска снималась с цилиндра, то исходный текст превращался в беспорядочный набор букв.

17 *Бэкон Ф.* Указ. соч. С. 324.

18 Там же. С. 323.

содержит 510 букв, то есть в 5,6 раз больше символов, чем необходимо для шифрования содержания *внутреннего письма*. Следовательно, конец *внешнего письма* является *пустышкой*, не несущий секретного послания.

Данный пример нами приведен не случайно. Именно в него и вкрались ошибки, допущение в академическом издании трудов Ф. Бэкона в конце прошлого столетия, хотя типографское искусство со времен ученого возросло многократно. Дело, увы, не в типографских ошибках и опечатках (которых, заметим, все-таки удалось избежать самому Бэкону при первом издании его труда).

Анализ ошибок, вкравшихся в текст академического издания

Во второе, исправленное и дополненное издание сочинений Ф. Бэкона (как, впрочем, и в первое) вкрались досадные ошибки, касающиеся его *двухлитерного шифра*. Насколько известно автору, других академических изданий трудов Бэкона в нашей стране предпринято не было. Данные ошибки (разного характера) искажают мысль английского философа о «высшей ступени совершенства шифра»[19]. Попробуем разобраться, почему это произошло, и внесем необходимые исправления.

«Лесами символов бредет, в их чащах тонет // Смущенный человек»[20]. Наверное, нечто подобное и произошло с редактором-философом, который работал над этим разделом трактата Бэкона. Уделив все свое внимание другим аспектам текста, «в чаще символов» шифра он, видимо, не смог до конца разобраться. Тем более, как будет показано ниже, начало дешифровки не осложнено никакими трудностями. Как видно из табл. 2, только с 34-й буквы *скрытого* послания (которая соответствует 34-й пятибуквенной группе в *открытом* тексте) начались проблемы дешифровки.

В табл. 2 текст *внешнего письма* для удобства исследования разбит на пятибуквенные группы, которые пронумерованы по краям таблицы. По левому краю таблицы сверху вниз идет отсчет десятков, а сверху таблицы слева направо – единиц. В первой строке располагается текст (со всеми знаками препинания) отрывка из письма Цицерона, разбитый на пятибуквенные группы. Во второй строке таблицы пятибуквенные группы переведены в *символы* (буквы) *двухлитерного шифралфавита*. В третьей строке происходит дешифровка этих *символов* согласно табл. 1. Дешифрованные буквы записаны прописью. Некоторые из букв в данной строке помечены верхним индексом, который означает номер ошибки, рассматриваемой нами далее. Неправильно дешифрованные буквы выделены также *курсивом*. Прочерк означает, что дешифровка невозможна, так как нет соответствующей замены в исходном шифре (см. табл. 1). Для удобства сравнения в четвертой строке приведено секретное дешифруемое послание спартанцев, в котором в целях наглядности выделены двойной рамкой отдельные слова. При правильной дешифровке третья и четвертая строка должны совпасть.

---

[19] *Бэкон Ф.* Указ. соч. С. 323.

[20] *Бодлер Ш.* Сплин и идеал, IV («Соответствия») Пер. Эллиса (Л. Кобылянского) // *Бодлер Ш.* Цвет зла: Стихотворения. СПб., 2009.

Таблица 2

Дешифровка отрывка из письма Цицерона

	1	2	3	4	5	6	7	8	9	10
0	E**go o**m	ni **o**ff	**i**cio, a	c po**ti**	**u**s pie	**t**a**te** e	rga te,	ca**e**te	**r**is sa	tisfa
	abbba	*aabaa*	*baaaa*	*aaabb*	*abaaa*	*baaba*	*aaaaa*	*aabaa*	*baaaa*	*aabaa*
	P	E	R	D	I	T	A	E	R	E
	P	e	r	d	i	t	a	e	r	e
10	**c**io o**m**	**nibus**:	**mihi** i	**pse** nu	nqu**am**	satis	**f**acio.	**Tanta**	**e**st e**n**	im ma**g**
	baaab	*ababb*	*abaaa*	*abbaa*	*aaabb*	*aaaaa*	*baaaa*	*baabb*	*baaab*	*aaaba*
	S	M	I	N	D	A	R	V	S	C
	s:	M	i	n	d	a	r	u	s	c
20	ni**t**ud	o tu**or**	**um**, erg	a me **me**	**r**itor	**um**, **ut** q	**uonia**	m **t**u, ni	**si per**	**f**ecta
	aabaa	*aaaba*	*abaaa*	*aaabb*	*abaaa*	*babaa*	*ababb*	*abaaa*	*ababa*	*abaaa*
	E	C	I	D	I	T	M	I	L	I
	e	c	i	d	i	t:	m	i	l	i
30	**r**e, **de** m	e **no**n c	**o**nqu**i**	esti: e	**g**o, qu**i**	**a** no**n i**	**d**em in	t**ua** ca	**usa ef**	**fi**cio,
	baaba	*aabaa*	*baaab*	*aaaba*	*baaab*	*baabb*	*baaaa*	*abaaa*	*baabb*	*abbaa*
	T	E	S	*C*[1]	S	V	R	I	V	N
	t	e	s	e	s	u	r	i	u	n
40	**v**iti**u**	m **mi**hi	**esse** a	**cerbu**	**m** pu**te**	m. **I**n ca	us**a ha**	**ec** sun	t: **Am**mo	**nius** r
	baaba	*abbaa*	*abbaa*	*bbbbb*	*baabb*	*aabaa*	*aabbb*	*abaaa*	*abbaa*	*abbaa*
	T	N	*N*[2]	-	V	E	H	I	N	*N*[3]
	t:	n	e	q	u	e	h	i	n	c
50	eg**is l**	**e**gat**u**	s a**p**er	te **pec**	**u**n**ia** n	**os** opp	**ug**nat.	Res **a**g	itur p	**er** eos
	aabab	*baaab*	*aabaa*	*aabab*	*baaba*	*baaaa*	*abaaa*	*aaaba*	*aaaaa*	*baaaa*
	F	*S*	*E*	*F*	*T*	*R*	*I*	*C*	*A*	*R*
	n	o	s	e	x	t	r	i	c	a
60	de**m** cr	e**di**to	res, pe	r **quos**,	**c**um **tu**	adera	s, **ageb**	a**t**ur. R	egi**s** c	aus**a**, **s**
	aabaa	*abbaa*	*aaaaa*	*abbbb*	*baabb*	*aabaa*	*aabbb*	*abaaa*	*aaaba*	*aaabb*
	E	*N*	*A*	*Q*	*V*	*E*	*H*	*I*	*C*	*D*
	r	e,	n	e	q	u	e	h	i	c
70	i **q**ui s	**u**nt, **qu**	**i** ve**l**i	n**t**, qui	**p**au **ci**	**s**unt, **o**	m**nes a**	d Pomp	**eium** r	em **d**ef
	abaaa	*baabb*	*baaba*	*abaaa*	*baabb*	*baaab*	*ababb*	*aaaaa*	*abbaa*	*aabaa*
	I	*V*	*T*	*I*	*V*	*S*	*M*	*A*	*N*	*E*
	d	i	u	t	i	u	s	m	a	n
80	**e**rri v	ol**u**nt.	**Sena**t	us **rel**	**igion**	**is** ca**l**	**u**mn**ia**	**m**, no**n r**	**eligi**	**on**e, s**e**
	baaaa	*aabaa*	*abbba*	*aabab*	*baabb*	*bbaab*	*baabb*	*baabb*	*baaab*	*bbaab*
	R	*E*	*G*	*F*	*V*	-	*V*	V	*S*	-
	e	r	e	p	o	s	s	u	m	u
90	**d m**ale	**volen**	tia, **et**	**illiu**	s **regi**	ae **l**ar	**gi**tio	**nis** in	**vidia**,	com**pr**
	bbaaa	*babbb*	*aaabb*	*babaa*	*ababa*	*aabaa*	*bbaaa*	*abbaa*	*baabb*	*aaabb*
	-	*Z*	*D*	*W*	*L*	*E*	-	*N*	*V*	*D*
	s.									
100	**ob**at, e	tc.								
	bbaaa	**-**								
	-	-								

Первая опечатка (но не ошибка) находится в 34-й пятибуквенной группе (или другими словами в 34-й букве зашифрованного текста). Вместо ожидаемой буквы E (*aabaa*) на этом месте стоит буква C (*aaaba*). Здесь мы имеем дело с простой опечаткой, возникшей при наборе (так как в этой группе соседние *символы a* и *b* «нечаянно» поменялись местами): слово «**co**nqu**i**es**ti**» должно было быть напечатано как «**co**nqu**i**es**TI**» (здесь и далее большими

буквами выделены необходимые исправления). Примечательно, что в оригинале трактата Бэкона[21] (см. рис. 1) этой опечатки нет. В начале шестой строки страницы оригинала ясно видно, что «**t**» имеет завитушку, плавно переходящую от низа буквы к ее «перекладине». По контрасту с другими, более строгими «t» данная буква является буквой алфавита с **полужирным** начертанием. А вот «i» имеет округлость внизу (не такую острую, в отличие от «**i**» «второго» шрифта). Очевидно, что эта буква принадлежит алфавиту с обычным начертанием.

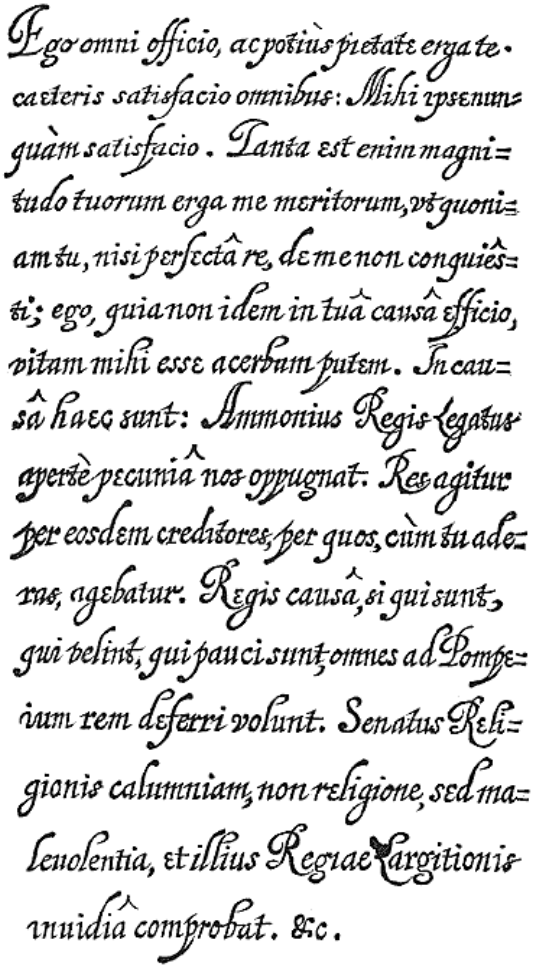
Ego omni officio, ac potiùs pietate erga te. cæteris satisfacio omnibus: Mihi ipsenunquàm satisfacio. Tanta est enim magnitudo tuorum erga me meritorum, vt quoniam tu, nisi perfectâ re, de me non conquiêsi; ego, quia non idem in tuâ causâ efficio, vitam mihi esse acerbum putem. In causâ hæc sunt: Ammonius Regis legatus apertè pecuniâ nos oppugnat: Res agitur per eosdem creditores, per quos, cùm tu aderas, agebatur. Regis causâ, si qui sunt, qui velint, qui pauci sunt, omnes ad Pompeium rem deferri volunt. Senatus Religionis calumniam, non religione, sed malevolentia, et illius Regiæ largitionis invidiâ comprobat. &c.

Рис. 1. Отрывок, зашифрованный методом Ф. Бэкона, из письма Цицерона с *внутренним* скрытым *посланием* воинов Спарты из первого издания трактата «О достоинстве и преумножении наук»

По всей вероятности, история этой опечатки восходит к тем временам, когда впервые заменили оригинальные шрифты Бэкона на более строгие шрифты с «современными» начертаниями (к примеру, обычными и **полужирными**) букв алфавита. Отметим, что идея двухлитерного шифра Бэкона, в котором каждый из двух применяемых алфавитов едва отличим от другого для непосвященного читателя, сработала и привела к рассматри-

[21] *Bacon F.* Opera. T. I: Qui continet “De dignitate et augmentis scientiarum” libros IX. Londini, 1623. P. 282.

ваемой опечатке. Как видим, кто-то недоглядел мелкие детали шрифтов в этих «алфавитах» (или вовсе не обратил на них внимания) при очередном издании трудов философа.

Вторая ошибка вкралась в 43-ю и 44-ю группы букв, во фразу «e**ss**e a**cerbum**». Интересно отметить, что 44 группа состоит из символов *bbbbb*, соответствия которому нет в алфавите шифра (см. табл. 1)! После чего текст ненадолго выправляется (в данном случае это просто счастливая случайность) с 45-й по 49-ю группу. Далее он снова портится (исключая случайное совпадение для буквы V в 88-й группе) уже вплоть до самого конца (91-я группа) дешифруемого текста. Тем не менее *открытый* текст («*внешнее письмо*» или отрывок из первого письма Цицерона) продолжается до 102-й группы, но уже является *пустышкой*, не несущей зашифрованную информацию. Касательно 43-й группы вопрос, кажется, может быть легко решен. Здесь получилась буква N (*abbaa*) вместо необходимой E (*aabaa*). Достаточно заменить только вторую букву *b* в последовательности на *a*, то есть вместо «e**ss**e» написать «e**S**s**e**».

А в 44-й группе *bbbbb* должна находится буква Q (*abbbb*). Как видим, здесь не совпала всего лишь одна первая буква. Выход тот же: заменить «a**cerbum**» на «a**C**e**rbum**».

Вроде бы у нас снова две ошибки-опечатки, такие же, как и в первом случае, тем более, что в дальнейшем текст как будто выравнивается. Но это вовсе не так.

Достаточно посмотреть внимательнее на оригинал трактата с этой страницей (рис. 1). В седьмой строке у Бэкона написано: «жизнь кажется мне горькой» – “**v**it**a**m m**ih**i ess**e** ace**rbam**” (*baaba abbaa aabaa abbbb*), а в академическом издании сочинений мы уже читаем с 41-й группы: «**ви**на кажется мне горькой» – «**v**it**i**um **mi**hi e**ss**e a**cerbum**» (*baaba abbaa abbaa bbbbb b*)[22]. Что же произошло? Первые две группы (41 и 42) совпадают (поэтому совпали и буквы T и N в проводимой дешифровке с буквами на тех же местах в уже известном нам послании спартанцев), а последние две (43 и 44) мы уже обсудили выше. Но в академическом тексте эта фраза содержит на одну букву больше! Отсюда и все дальнейшие ошибки. Это была бы простая опечатка, если бы дешифруемый текст далее выравнивался не только по 49-ю группу (как это случайно произошло здесь, и закономерно – при *первой опечатке* в 34-й группе), а восстановился бы целиком до самой последней группы.

[22] *Бэкон Ф.* Указ. соч. С. 325.

Таблица 3

Сравнение слов в письме Цицерона, соответствующих отрывку “t: neque hinc” внутреннего письма спартанцев, из академического издания и первого издания трактата Ф. Бэкона

	Академическое издание, 1977 г.									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
40	**vit**i**u**	m **mi**hi	**ss**e a	**cerbu**	**m** pu**te**	m. I**n** ca	us**a ha**	**e**c sun	t: **Am**mo	n**i**u**s** r
	baaba	*abbaa*	*abbaa*	*bbbbb*	*baabb*	*aabaa*	*aabbb*	*abaaa*	*abbaa*	*abbaa*
	T	N	N^2	-	V	E	H	I	N	N^3
	t:	n	e	q	u	e	h	i	n	c
	Первое издание трактата, 1623 г.									
	vita**m**	m**ih**i e	ss**e** ac	**erbam**	**p**ut**em**.	In **c**au	sa **hae**	c **s**unt:	A**mm**on	ius **r**e
40	*baaba*	*abbaa*	*aabaa*	*abbbb*	*baabb*	*aabaa*	*aabbb*	*abaaa*	*abbaa*	*aaaba*
	T	N	E	Q	V	E	H	I	N	C
	t:	n	e	q	u	e	h	i	n	c

Из табл. 3 видно, что у второй ошибки в 43-й группе «длинные ноги»: она начинается аж в 41-й группе из-за того, что вместо слова “vitam” (жизнь), как в первом издании у Бэкона, в академическом издании написано “vitium” (вина, ошибка). Произошла смысловая подмена: «жизнь» была заменена на схожую по написанию «вину». Смысл написанного Цицероном от этой замены сильно не пострадал. Нельзя думать, что в философской редакции издательства решили таким образом «подправить» мастера слова, блестящего оратора и философа, для которого латынь была родным языком.

Различие в одной букве между “acerb*u*m” (*лат.* ʿгорькийʾ) и “acerb*a*m” (не приведшее к искажению в дешифровании) связано не с очередной опечаткой, а со склонением прилагательных разного рода. Так, в аккузативе (винительном падеже) при склонении прилагательных в среднем роде используется окончание -*u*m («вина» в латыни ср. рода, номинатив vitium), а в женском – -*a*m («жизнь» в латыни жен. рода, номинатив vita). Данное различие в окончаниях еще раз указывает на то, что источник отрывка, из которого было взято письмо, разнится с текстом Бэкона.

Вернемся еще раз к этой смысловой ошибке. Для шифра было неважно, что слово написано с небольшими искажениями (по смыслу или по норме); искажение в шифр внесло только то, что это слово было всего лишь на одну букву длиннее, чем то, которое использовал Бэкон. Если бы они совпадали по длине, то мы вообще ничего бы не заметили при дешифровке. Но мы это заметили в 50-й группе (напомним, что ошибка была совершена в 41-й группе).

А что же было с исследуемым нами отрывком при первом издании сочинений философа? Напомню, что ранее мы цитировали исключительно по второму, исправленному и дополненному изданию.

В первом издании мы можем прочесть “**vit**i**a**m **mi**hi e**ss**e a**cerbam**”[23]. Как видим, это нечто среднее между бэконианской версией “**vit**a**m**” и академической версией “**vit**i**u**m”. Фактически ничего не изменится в нашем анализе

[23] *Бэкон Ф.* Соч.: 2 т. Т. 1. М., 1971. С. 340.

дешифровки академической версии фразы, проведенной по второму изданию сочинений: выделенные полужирным начертанием буквы стоят на тех же самых местах и длина фраза осталась прежней (на одну единицу больше оригинальной версии). Поэтому все ошибки останутся на своих местах. Но зато теперь видна работа редактора по «исправлению» этого отрывка. В текст вкралась всего лишь одна лишняя буква – i: “**v**it**a**m” превратилась в другое осмысленное слово “**v**it**i**am”, но при этом поменялся род. Редактор второго издания заметил, что окончание в аккузативе для этого слова здесь ошибочно, и исправил его вместе с соответствующим ему прилагательным на “**v**it**i**um <...> a**cerbum**”. На этом правка была завершена: нормы классической латыни восторжествовали. Но, увы, отнюдь не все точки над *i* были расставлены по своим местам. Произошла незаметная для глаза редактора, но с точки зрения криптоаналитика вопиющая «криптографическая катастрофа».

Рассмотрим внимательнее «*третью ошибку*» в 50-й группе. Именно как об ошибке о ней можно было бы говорить, если бы мы думали, что *вторая* указанная нами *ошибка* является простой опечаткой. Текст дешифровки после второй ошибки на недолгое время «выпрямился» и окончательно «испортился» именно в этой группе. Что же мы здесь видим? Вместо ожидаемой буквы C (*aaaba*) на этом месте стоит N (*abbaa*). Если ошибка, возникшая в первом случае, является опечаткой, а во втором случае ловко маскируется под нее, то здесь говорить об опечатке трудно – не совпадают (по местоположению) целых три буквы (со второй по четвертую). Даже их исправление ничего не дает, так как в последующих группах мы столкнемся с такими же проблемами. Но при исправлении второй ошибки все эти трудности исчезнут сами собой: текст будет полностью успешно дешифрован и совпадет с ответом, который приводит Бэкон.

Случайное совпадение буквы V (88-я группа) в уже неправильно дешифруемой цепочке букв текста с истинным значением этой группы дает нам повод для короткого математического отступления в *теорию вероятностей*. «Сбитая» цепочка содержит (с 50-й по 91-ю группу) 42 буквы. Напомним, что во *внутреннем письме* ровно 91 буква. То есть около 46 %, исключая опечатки, дешифровки неверно. Поэтому вполне ожидаемо, что среди 42 букв одна может оказаться случайным образом верной. Гораздо труднее ожидать, что в подобной цепочке окажутся верными целых пять идущих подряд букв. Тем не менее именно такое примечательное с точки зрения *теории вероятностей* событие произошло с 45-й группы по 49-ю (ведь настоящий сбой в шифре, напомним, произошел уже в 41-й группе).

Заключение или «Instauratio magna»[24]

Ниже приведен исправленный с учетом вышесказанных замечаний отрывок из письма Цицерона, приводимый в качестве примера Бэконом. Так как с течением времени краска на бумаге выцветает, буквы затираются от частого или неряшливого использования книги, то подчеркивания различий в *двухлитерном шифре* только выделением букв с помощью **полужирного** начертания недостаточно. Ярким примером этого служит академическое издание: в нем разве только тщательно приглядываясь, иногда при помощи лупы (и все еще

[24] «Великое восстановление наук» – заглавие неоконченного трактата Ф. Бэкона; его первая часть («Новый органон») была опубликована в 1620 г. Отсюда: «Великое восстановление» (“Instauratio magna”).

сомневаясь), можно различить, что буквы набраны **полужирным** начертанием. Ведь они так похожи на своих соседок, набранных обычным шрифтом! Конечно, Бэкон бы порадовался, что его «маскирующийся» шифр сработал. Но представляется, что в академическом издании важно было бы подчеркнуть мысль ученого и сделать различия двух шрифтов более явными, как это сделал сам философ при первом издании своего труда (см. рис. 1). Поэтому ниже одна часть *двухлитерного алфавита* набрана *курсивными* буквами, вторая же выделена **полужирным** начертанием и ПРОПИСНЫМ написанием букв. Тогда исправленный латинский текст письма принимает следующий вид:

«*E***GO O***mni* **O***ff***I***cio*, *ac po***TI***u***S** *pie***T***at***E** *erga te*, *ca***E***te***R***is sati***S***fa***C***io o***M***n***I***-b***US*: *m***I***hi ip***SE** *nunqu***AM** *satis***F***acio*. **T***an***TA E***st e***N***im m***A***gni***T***udo tu***O***ru***M**, *erga me* **ME***r***I***tor***U***m*, **U***t qu***O***n***IA***m* **T***u*, *nis***I** *p***E***rf***E***cta* **R***e*, *d***E** *me n***O***n c***O***nqu***I***es***T***i*: *e***G***o*, *qu***IA** *no***N ID***em in t***U***a ca***U***sa* **EF***f***IC***io*, **V***it***A***m m***IH***i ess***E** *ace***RBAM P**ut**EM**. *In* **C***ausa* **HAE***c* **S***unt*: *A***MM***onius* **R***eg***IS** *leg***AT***u***S A***per***T***e p***E***cu***N***i***A** *n***OS** *op***P**u**G**-nat. *Re***S** *agitur* **P***er eosd***E***m credi***T***ore***S**, **P***er qu***O***s*, *cu***M TU AD***er***AS**, *ag***E***batu***R**. **RE***g***I***s causa*, **S***i qui* **SU***n***T**, *qui* **V***el***INT**, *qu***I** *pa***U***ci s***U***nt*, **OMN***es a***D** *P***O***m***PE***ium rem* **DE***ferr***I** *vo***L***unt*. *Sen***A***tus* **RE***L***I***g***IO***n***IS** *ca***LUM***nia***M**, **N***on* **RE***l***I***g***ION***e*, *s***ED M***ale***V***o***L***ent***I***a*, **E***t* **I***/***L***ius* **R***e***G***iae* **L***ar***GI***tion***IS** *in***V***id***IA**, *com***PRO***bat*, *etc*.»

Конец отрывка «*o***L***ent***I***a*, **E***t* **I***/***L***ius* **R***e***G***iae* **L***ar***GI***tion***IS** *in***V***id***IA**, *com***-PRO***bat*, *etc*.» представляет собой *пустышку*, не несущую текста *внутреннего письма*. Тем не менее она дешифруется как «IXIWKSTNP-». Увидав эту бессмыслицу, дешифровщик отбросит ее от основного послания, как теперь уже ненужный довесок, который сыграл свою роль и скрыл наличие самого шифра (и тем самым еще раз обезопасил *внутреннее* секретное *письмо*).

Список литературы

Бэкон Ф. Соч.: 2 т. Т. 1 / Под ред. А.Л. Субботина. М.: Мысль, 1971. 592 с.

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.

Цицерон М.Т. Письма. Т. 1: Годы 68–51 / Пер. с лат. В.О. Горенштейна. М.; Л.: Изд-во АН СССР, 1949. 536 с.

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

Pesic P. The clue to the labyrinth: Francis Bacon and the decryption of nature // Cryptologia. 2000. Vol. XXIV. № 3. P. 193–211.

On Bacon's biliteral cipher

Ivan Efishov

PhD in Physics and Mathematics, Associate Professor of Computer Security. Immanuel Kant Baltic Federal University. 14 Alexander Nevsky Str., Kaliningrad, 236016, Russian Federation; Senior Research Fellow. Kaliningrad Branch of Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation of the Russian Academy of Sciences. 41 Pobedy ave., Kaliningrad, 236010, Russian Federation; e-mail: IEfishov@kantiana.ru

In the second, revised and expanded edition of the works of Francis Bacon published under the auspices of the Institute of Philosophy of the Academy of Sciences of the USSR almost thirty years ago (1977), annoying errors of cryptographic nature were made in Chapter I,

Book VI of the treatise *On the Advancement of Learning*. All of them relate to the biliteral cipher invented by Bacon, according to his own statement, in his youth. These errors (which are of various origin) misrepresent what the English philosopher and statesman, founder of empiricism has to say about "the highest degree of cypher", known today as Bacon's cipher (or code). They also deprive of any value the examples carefully chosen by Bacon for this late work. It is worth noting that in the first lifetime edition of this work in Latin (1623) none of the said errors is present, which means that the author was more concerned with the correct reproduction of his text than the philosophical supervisors of an edition which was to be printed more than three hundred and fifty years later. Now the sequence of symbols 0 and 1 (or, in Baconian terms, of the "two letters" *a* and *b*) is a binary sequence of the kind which makes possible the operation of all modern computers. It looks like Bacon foresaw a great future for such method of transmitting information: "Neither is it a small matter these *Cypher-Characters* have, and may perform: For by this *Art* a way is opened, whereby a man may express and signify the intentions of his mind, at any distance of place, by objects which may be presented to the eye, and accommodated to the ear". Unfortunately, no one, let alone a philosopher, is immune to mistakes committed against his work by others. The purpose of this article is to trace down such mistakes, typographical errors included, and to suggest the necessary amendments to the Russian text of the respective chapter of the treatise *On the Advancement of Learning*.

Keywords: Francis Bacon, biliteral cipher, cipher, binary code

References

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

Bacon, F. *Sochineniya* [Selected Works], Vol. 1, ed. by A. Subbotin. Moscow: Mysl' Publ., 1971. 592 pp. (In Russian)

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)

Gorenshtein, V. (tr.) Cicero, *Pis'ma* [The Letters], Vol. 1. Moscow; Leningrad: AS USSR Publ., 1949. 536 pp. (In Russian)

Pesic, P. "The clue to the labyrinth: Francis Bacon and the decryption of nature", *Cryptologia*, 2000, Vol. XXIV, No 3, pp. 193–211.