

РАСШИФРОВКА ДВУХ ТЕЛЕГРАММ ИЗ ДЕЛА ПО УБИЙСТВУ ЦАРСКОЙ СЕМЬИ

Иванов А.Р. Email: Ivanov6102@scientifictext.ru

Иванов Артур Рейнович - инженер-электронщик и программист,
ООО «Тахион», г. Петрозаводск

Аннотация: статья описывает расшифровку двух телеграмм из материалов следствия по убийству Николая II и его семьи, инициированного в 1918-м году военными властями Белой армии. В рамках этого следствия секретная переписка Уралсовета с Москвой была раскрыта старшим лейтенантом А.А. Абаза еще в 1920-м году, но две зашифрованные телеграммы из Екатеринбурга в Пермь оставались не прочитанными на протяжении более 100 лет и будоражили умы исследователей, полагающих в них великую сокрытую тайну. Их расшифровка казалась не достижимой в силу убийственной краткости содержащегося в них текста, исключавшей применение известных статистических методов и оставлявшей слишком большой простор для неопределенности. Автору статьи удалось раскрыть содержание этих телеграмм благодаря тому, что полученный чисто математически результат содержал лакуны, однозначным образом заполняемые сопоставлением с историческими лицами и событиями, и показать, что эти телеграммы прямого отношения к убийству царской семьи не имеют.

Ключевые слова: история криптографии, советские шифры, убийство Николая II, убийство царской семьи, зашифрованные телеграммы.

DECRYPTION OF TWO TELEGRAMS FROM THE CASE PAPERS ON THE MURDER OF NICHOLAS II AND HIS FAMILY Ivanov A.R.

Ivanov Arthur Reynovich - electronic Engineer and Programmer,
Co. Ltd. «TACHYON», PETROZAVODSK

Abstract: the article describes the decryption of two telegrams from the case papers on the murder of Nicholas II and his family. As part of investigation initiated in 1918 by the military authorities of the White Army, the secret correspondence of the Uralsovet with Moscow was deciphered by A. A. Abaza back in 1920, but two encrypted telegrams from Yekaterinburg to Perm remained unread for more than 100 years and excited the minds of researchers who saw them as a great hidden secret. Their decryption did not seem real due to the extremely brevity of the text contained in them, which excluded the use of well-known statistical methods and left too much room for uncertainty. The author of the article managed to reveal the content of these telegrams due to the fact that the result obtained purely mathematically contained lacunae, unambiguously filled by matching with historical persons and events, and showed that these telegrams are not directly related to the murder of the royal family.

Keywords: history of cryptography, soviet ciphers, murder of Nicholas II, encrypted telegrams.

УДК 003.26

Материалы расследования убийства Николая II и его семьи, которое в 1918-м году было инициировано военными властями Белой армии и проводилось последовательно следователями Д.А. Малиновским, А.П. Наметкиным и А.Ф. Кирста, И.А. Сергеевым и в дальнейшем вплоть до своей смерти в 1924-м году Н.А. Соколовым, опубликованные в сборнике документов "Гибель царской семьи. Материалы следствия" под редакцией Н. Росса [2], содержат три зашифрованные телеграммы, содержание которых на протяжении более чем 100 лет оставалось не известным. Автору статьи удалось расшифровать две из них, а именно телеграммы со страниц 214 и 216 сборника Росса.

Обе телеграммы оказались зашифрованы шифром омофонической замены, так называемым "квадратным шифром" [4], с использованием одного и того же шифровального квадрата. Восстановленная часть шифровального квадрата выглядит так:

Таблица 1. Шифровальный квадрат

	0	1	2	3	4	5	6	7	8	9
0			В					Е		
1		э	К	С	Д		х	т	р	
2		Л		О	б	Н			С	а
3	ы	б	Е		И	К	п	У	к	Т
4						д		А		В
5	ь		М	Р	Е		И	й	Т	

<i>б</i>		<i>Л</i>		<i>б</i>	<i>ц</i>	<i>ш</i>		<i>з</i>		<i>Н</i>
<i>7</i>	<i>ю</i>	<i>А</i>		<i>х</i>	<i>О</i>	<i>г</i>	<i>И</i>			<i>р</i>
<i>8</i>		<i>м</i>	<i>о</i>	<i>С</i>	<i>В</i>		<i>ы</i>			<i>Д</i>
<i>9</i>		<i>Е</i>			<i>Я</i>	<i>й</i>		<i>Л</i>		

Расшифровывание производилось разбиением шифрограммы на последовательность двузначных чисел и поиском соответствующих числам букв в квадрате. При этом десятки чисел определяли строку, а единицы столбец квадрата.

Пустые клетки квадрата соответствуют значениям оставшимся не известными, соответствующие им двузначные числа в телеграммах не встретились. Приведенные прописными буквами значения установлены надежно и перекрестно проверены взаимным соответствием в разных местах телеграмм. Помеченные строчными буквами значения встретились в обеих телеграммах только один раз, т.е. получены предположением смысла текста. При этом, в силу того, что в шифрограммах мог использоваться усеченный до 27 букв алфавит [4], возможно, что строчные "й" и "ы" в квадрате на самом деле "и", а строчная "э" на самом деле "е".

Приведенным шифровальным квадратом были расшифрованы следующие телеграммы:

Телеграмма 1.

7 июля 1918 года

Из Екатеринбурга в Пермь, Военком Лукоянову.

94182 31321 29022 10712 37144 71361 32453 75439 52713 94932

54844 97467 83587 12576 91635 49782 75844 75389 54766 49102 точка

12713 58454 89375 88354 24944 97165 56615 44930 07112 89479 86

номер

Белобородов [2, с.214].

расшифровалась как

ЯРОСЛАВЛЕКУДАСЛЕДУЕТМАТВЕЕВВОЗСТАНИЕБЕЛОГВАРДЕИЦЕВ.

КАКВЕДУТСЕБЯВАШИЛЕВЫЕЭСЕРЫ

Телеграмма 2.

9 июля 1918 года

Из Екатеринбурга в Пермь, Военком Лукоянову.

73231 73452 28355 69528 76699

44913 38565 73732 16719 73436

91538 15037 83584 76974 02765

85425 71319 77014 91697 607

номер 8818. Белобородов

№ 4653 [2, с.216].

расшифровалась как

ХОТИМСКИЙСИНЯВСКИЙУЕХАЛИПЕРМЬУСТАНОВИТЕНАБЛЮДЕНИЕ

Анализ надежности расшифровки

Представим расшифрованные тексты обеих телеграмм таким образом:

ЯрОСЛаВЛЕКУДАСЛЕДУЕТМАТВЕЕВВОзСТАНИЕБЕЛОгВАРДЕИцЕВ.

КАКВЕДУТСЕБЯВАшИЛЕВЫЕЭс?ры

хОтИМСКийСИНЯВСКийУЕхАЛИпЕРмьУСТАНОВИТЕНАбЛюдЕНИЕ

где прописными буквами пометим надежно установленные буквы, перекрестно проверенные их появлением в разных местах телеграмм, строчными буквами пометим буквы, соответствующие двузначным числам, встретившимся в телеграммах только один раз, т.е. полученные предположением и знаком вопроса выделим букву, соответствующую предполагаемой опечатке в телеграмме. В данном случае опечатка состоит в том, что группа цифр 89479 первой телеграммы должна быть исправлена в единственной цифре на 85479, с опечаткой в расшифровке получается "эСЯры", после исправления "эСЕРы".

Опечатки по одной цифре на телеграмму можно найти в других шифрованных телеграммах, приложенных к делу об убийстве царской семьи, можно даже сделать предположение, что такие опечатки могли быть определенным условным знаком. В частности, в телеграмме от 26 июня 1918 г. № 4323 из Екатеринбурга в Москву от Белобородова Горбункову [2, с.260], зашифрованной шифром Виженера с ключом "ЕКАТЕРИНБУРГ" [4, ч. 3, гл. 13], в группе цифр 2 5 4 3 8 0 5 2 восьмерка должна быть заменена на двойку, иначе двузначное число 80 выбьется из обязательного в используемом шифре диапазона 01..54, а после такой замены телеграмма расшифровывается безупречно. Т.е. в данном случае опечатка в одной цифре несомненна. Поэтому и при расшифровке других телеграмм разумно предполагать возможность отдельной опечатки.

Формально оценивая результат можно заметить, что во второй телеграмме "уехали/в/Пермь" допускает прочтение "уехали/из/Перми" (окончание слова Пермь - результат предположения), однако

такое прочтение разрушает смысл телеграммы из Екатеринбурга в Пермь (если бы упоминаемые Хотимский и Синявский уехали из Перми, то телеграмма об этом скорее полетела бы в обратном направлении) и кроме того предложенная расшифровка "/в/Пермь" соответствует событиям. Упомянутые в телеграмме Хотимский и Синявский это очевидно Валентин Иванович Хотимский (1892-1937) и отец известного в будущем диссидента Донат Евгеньевич Синявский (1895-1960), оба лидеры уральских левых эсеров. Чтобы подкрепить прочтение "/в/Пермь" необходимо проверить вектор их перемещения в Пермь. Но этот вектор именно таков, потому что по воспоминаниям председателя Уралоблсовета А.Г. Белобородова В.И. Хотимский участвовал в выборе особняка Ипатьева для содержания царской семьи [3, с.243], следовательно весной 1918-го находился в Екатеринбурге, а вот осенью 1918-го он вместе с Д.Е. Синявским находился в Перми [1]. Кроме того известно в связи с какими обстоятельствами Д. Е. Синявский попал в Пермь: Д.Е. Синявский возглавлял отряд из 40 человек, в основном левых эсеров, который сопровождал в Москву эшелон с ценностями, эвакуируемыми из Екатеринбургского монетного двора, но в связи с белогвардейским восстанием в Ярославле эшелон был вынужден вернуться в Пермь [5]. Это произошло в те же дни, что и отправка второй телеграммы. Поэтому прочтение в ней "уехали/в/Пермь" убедительно обосновано.

Аналогично, формально оценивая результат, можно заметить, что слово "эсеры" в первой телеграмме имеет большую неопределенность (одна буква в нем - результат предположения об опечатке, а три - результат просто предположения), но эта телеграмма была отправлена ровно на следующий день после убийства немецкого посла Мирбаха и мятежа левых эсеров в Москве, поэтому вопрос в ней о том как ведут себя левые эсеры в Перми выглядит самым актуальным. Более того совершенно естественным выглядит указание установить наблюдение за лидерами местных левых эсеров во второй телеграмме, отправленной через два дня после мятежа левых эсеров в Москве. Поэтому прочтение в первой телеграмме "левые эсеры" выглядит почти неизбежным.

Также, стоит отметить, что содержимое первой телеграммы не только подтверждается действительным фактом Ярославского восстания накануне отправки телеграммы, но и абсолютно стыкуется с содержимым нешифрованной телеграммы, отправленной непосредственно перед ней. Вот этой телеграммы:

07 июля 1918 года

№ ? из Екатеринбурга в Пермь, от Белобородова Лукоянову.

Пермь Лукоянову и Матвееву 2 адреса Королевские номера Сыромолотову

Если поезд Матвеева еще не отправлен то задержите запятая если отправлен принять все меры к тому чтобы он был задержан в пути и в коем случае не следовал месту указанному нами точка Случае ненадежности нового места стоянки поезд вернуть Пермь. Ждите шифрованную.

Белобородов [2, с. 214].

По сути, посланная следом за нешифрованной шифрованная телеграмма поясняла причину необходимости задержать поезд Матвеева.

Выводы

Несмотря на свою убийственную краткость, исключаящую применение статистических методов криптоанализа, при отсутствии дополнительного шифротекста из той же переписки, две из трех загадочных телеграмм из материалов белогвардейского следствия по убийству царской семьи поддались расшифрованию. Автором изложены все сомнительные моменты расшифровки и показано каким образом разрешалась их сомнительность. Поскольку результат расшифрования телеграмм железным образом сопрягся и с происходившими в то время событиями и с текстом сопутствующей не шифрованной переписки, полученное прочтение можно считать несомненным. К сожалению, оно никоим образом не оказалось связанным с убийством царской семьи и потому не пролило на эти события какой-либо дополнительный свет. В итоге, в деле об убийстве царской семьи осталась единственная телеграмма (в Надеждинск Андрееву [2, с. 217]), зашифрованная совершенно обособленным образом, открытый текст которой остается не известным и которая может содержать хоть какие-то новые сведения по делу.

Список литературы / References

1. ГАПК, ф. Р-732, д. 217, л. 7-8.
2. Гибель царской семьи. Материалы следствия. Франкфурт-на-Майне Посев, 1987, составитель Николай Росс.
3. Из воспоминаний председателя Уралоблсовета А.Г. Белобородова [Декабрь 1923 г.] // Скорбный путь Романовых, 1917-1918 гг. Гибель царской семьи: Сборник документов и материалов. Отв. ред. и сост. В.М. Хрусталева, при участии М. Д. Стейнберга. Москва: РОССПЭН, 2001.

4. *Синельников А.В.* Шифры и революционеры России. [Электронный ресурс] // ХРОНОС – всемирная история в интернете. Режим доступа: http://www.hrono.ru/libris/lib_s/shifr00.html/ (дата обращения: 15.03.2020).
5. *Фомичев И.А.* Надеждинские вооруженные формирования в годы Гражданской войны. // Гражданская война на Урале: Материалы конференции, Екатеринбург, 2012.