

**Криптологическая деятельность
Особого отдела Департамента полиции в начале XX века
Пылаева Евгения Ивановна¹**

студентка

*Вологодский государственный педагогический университет, исторический факультет,
Вологда, Россия*

E-mail: evgenia11_88@mail.ru

Введение

Термин «криптография» (греч. *kryptō* – тайный, скрытый + *graphō* – пишу) буквально переводится как «тайнопись» и в широком смысле трактуется как отрасль знания, изучающая системы тайнописи. В более узком и прикладном смысле под *криптографией* следует понимать совокупность методов системного изменения формальной структуры текста с целью полностью или частично скрыть заложенную в нем информацию. Криптография как отрасль знания включает в себя некоторые специфические термины.

Исходным (открытым) текстом называется текст в его оригинальной форме, то есть структура и смысл данного текста могут адекватно восприниматься неограниченным кругом лиц. Под *криптограммой (шифртекстом)* понимается текст, получившийся в результате изменений, произведенных с помощью методов тайнописи. *Криптовеличина* — конечный структурный элемент исходного текста, который подлежит замене в процессе шифрования. Криптовеличиной, например, могут быть буквы, слоги, части слов. *Криптоединица* — структурный элемент криптограммы, который замещает криптовеличину в зашифрованном тексте. Наиболее часто криптоединицы имеют буквенное, числовое или символьное выражение. Криптоединицы могут как постоянными, так и переменными. Постоянный характер криптоединицы означает, что одной криптовеличине исходного текста соответствует криптоединица с одним и тем же значением либо графическим выражением. Переменными являются те криптоединицы, которые имеют несколько значений для одной и той же исходной криптовеличины. *Шифрalfавитом* называется определенный набор криптоединиц, необходимый для зашифровывания исходного текста. Термин «криптология» противоположен по значению термину «криптография». Под *криптологией* следует понимать совокупность методов, направленных на дешифрование закрытого текста (криптограммы) и выявления структурного и смыслового содержания искомого сообщения.

В последней четверти XIX – начале XX веков широкое распространение получила переписка, содержащая фрагменты зашифрованного текста. Данное явление объясняется новым подъемом революционных настроений в обществе и ответным усилением контроля политической полиции за деятельностью так называемых «неблагонадежных лиц». Среди методов борьбы политической полиции с набиравшим силу революционным движением одно из главных мест занимала перлюстрация, или тайное вскрытие частной корреспонденции, а также копирование письма или его части. Перлюстрированные письма, содержащие зашифрованный текст, направлялись из почтового отделения в Департамент полиции Министерства внутренних дел. Деятельность по дешифровке таких писем находилась в ведении V отделения Особого отдела Департамента полиции. Канцелярия V отделения фактически состояла из двух криптологов — И. А. Зыбина и его помощника С. И. Жабчинского, которые и выполняли всю работу по разбору зашифрованных писем. Копии дешифрованных ими писем рассылались далее по другим отделениям Особого отдела для их последующей разработки и ведения оперативно-розыскной деятельности по поступившей из данных писем информации.

¹ Автор выражает признательность А. В. Синельникову за помощь в подготовке тезисов.

Методы

В основу данного исследования положены историко-типологический и сравнительно-исторический методы и метод структурно-функционального анализа (СФА). Источниковую базу составляют документы из фондов Государственного архива Российской Федерации (ГАРФ) и Государственного архива Вологодской области (ГАВО). Источниковая база представлена в виде коллекции перлюстрированных писем, хранящихся в фонде Особого отдела Департамента полиции (ГАРФ. Ф. 102) и комплекса делопроизводственной документации Вологодского губернского жандармского управления (ГАВО. Ф. 108). Комплекс источников, непосредственно охваченных рамками данного исследования, составляют делопроизводственная переписка начальника Вологодского губернского жандармского управления (ВГЖУ) с Особым отделом Департамента полиции по поводу расшифровки писем и «уведомления об оказавшемся» и так называемые «разборы шифра», прилагавшиеся к деловым запискам, направленным из Особого отдела начальнику ВГЖУ для дальнейшей разработки сведений на местах.

Результаты

Проведенный анализ источников показал следующее: 1) в начале XX века наблюдалось стремительное усложнение формальной структуры шифров революционного подполья по сравнению с предыдущим периодом; 2) в указанный период выделяются две доминирующие качественные особенности данных криптосистем: многоалфавитность и усложнение структурной основы ключей к шифрам; 3) в указанный период появились сравнительно новые *символьные* криптосистемы, которые были основаны на использовании в качестве шифралфавита набора графических примитивов, структурно состоящих из различных комбинаций геометрических линий, точек и начертаний букв. В то же время источники свидетельствуют о том, что в XX века в криптологической деятельности V отделения Особого отдела наступил значительный спад, который был вызван не только стремительным совершенствованием техники шифрования в среде революционеров, но и отчасти был обусловлен увеличением в указанный период доли зашифрованных писем по отношению к общей массе перлюстрированной переписки. Таким образом, канцелярия V отделения к началу XX века перестала справляться с поставленными задачами, что в свою очередь свидетельствовало о наличии некоторого кризиса в деятельности всей политической полиции Империи и необходимости изменений в организации криптологической службы политического сыска России.

Подводя общий итог, мы можем заключить следующее: во-первых, криптологическая деятельность Особого отдела Департамента полиции представляет собой интересную и мало изученную страницу в истории политического сыска царской России и заслуживает более детального и широкого изучения; во-вторых, зашифрованная переписка представляет собой сложный, обладающий рядом специфических черт источник по истории революционного движения, который должен заслуживать не меньше внимания и интереса со стороны исследователей-историков, чем прочие.

Источники

1. ГАРФ. – Ф. 102. – Оп. 265 – Д. 1081. «Переписка Департамента полиции с начальником ВГЖУ о расшифровке и переводе писем разных лиц». – Л. 1 – 48.
2. ГАВО. – Ф. 108. – Оп. 1. – Д. 4247. «Переписка начальника ВГЖУ». – Л. 1 – 32.

Литература

1. Kahn D. (1967) The codebreakers. / D. Kahn. New-York, 1967.
2. Перегудова З. И. (2000) Политический сыск России, 1880-1917 / З. И. Перегудова. М. : РОССПЭН, 2000.
3. Саломая А. (1995) Криптография с открытым ключом / А. Саломая. М.: Мир, 1995.
4. Синельников А. В. (2000) Шифры и революционеры России /А. В. Синельников [Электронный ресурс]. Режим доступа: <http://hrono.rspu.ryazan.ru/avtory/sinelnikov.html>.