УДК 94.(47):351.741:625.1
doi 10.17072/2219-3111-2024-3-16-27
Ссылка для цитирования: *Колпаков П. А.* Тайнопись на стальных магистралях: перехват донесений, дешифровка и защита сведений железнодорожными жандармами // Вестник Пермского университета. История. 2024. № 3(66). С. 16–27.

ТАЙНОПИСЬ НА СТАЛЬНЫХ МАГИСТРАЛЯХ: ПЕРЕХВАТ ДОНЕСЕНИЙ, ДЕШИФРОВКА И ЗАЩИТА СВЕДЕНИЙ ЖЕЛЕЗНОДОРОЖНЫМИ ЖАНДАРМАМИ

П. А. Колпаков

Российский университет дружбы народов имени Патриса Лумумбы, 117198, Россия, Москва, ул. Миклухо-Маклая, 6
1kolpakov1@rambler.ru
ResearcherID: JGY-1738-2023
Scopus Author ID: 58657619800
SPIN-код: 1054-5704

Рассматривается деятельность жандармской железнодорожной полиции Российской империи по перехвату антиправительственной переписки и вражеских донесений, их дешифровке, защите информации о перевозках военных грузов на историческом интервале от последнего десятилетия XIX в. до Февральской революции. Обширный пласт ранее не опубликованной делопроизводственной документации жандармских полицейских управлений железных дорог позволил проанализировать примеры тайнописи (криптограмм), использовавшейся революционерами в России. В качестве недостатков применявшихся шифров определены наличие логической связи между буквами исходного текста и позициями в условных алфавитах, а также их устройство таким образом, что каждому шифруемому значению соответствует лишь одна позиция условного алфавита. Боевые группы политических радикалов активно стремились привлечь к сотрудничеству железнодорожных служащих и в особенности телеграфистов для получения и передачи сведений о следовании поездов с ценными грузами для планирования и реализации акций экспроприации. Критическая важность связи в годы Первой мировой войны повысила значимость шифровального дела и дешифровки (криптоанализа). Для шифровки сообщений о состоянии российских железных дорог противником использовался обширный арсенал приемов: замена ключевых слов в текстах установленными способами; применение шифрокниг, содержавших многообразные кодовые комбинации; сочетание замены значений и их перестановки по разработанным матрицам. Война дала импульс развитию тайнописи: с течением времени шифры усложнялись для раскрытия криптоаналитиками. Сокрытие содержания шпионских донесений обеспечивалось не только преобразованием текстов, но и изощренными методами упаковки носителей информации в багаже, среди продуктов питания, применением особых чернил. В ведении дешифровки железнодорожные жандармы в значительной степени были зависимы от особого отдела Департамента полиции МВД и Военного министерства. Эти ведомства предоставляли необходимые ключи. В свою очередь, железнодорожная жандармерия нарабатывала ценный опыт перехвата содержавших секреты писем при их перемещении по «чугунке».

Ключевые слова: железнодорожная жандармерия, тайнопись, шифр, шифрование, дешифровка, криптография, криптоанализ, Российская империя, Первая мировая война.

Введение

Противостояние сторон, одна из которых стремится сохранить пересылаемые секреты, а другая – перехватить и понять их содержание, раскрывается во всех критически важных для государства сферах: дипломатической, правоохранительной, научно-технической и, конечно, военной. В исторических трудах древних цивилизаций – Индии, Египта, Месопотамии – имеются сведения о системах и способах составления шифрованного письма. Традиции русского тайнописания уходят своими корнями в Средние века [*Соболева,* 2002, с. 6, 23]. Отправным моментом изучения в России шифрования как меры обеспечения государственных интересов является опубликованная в 1853 г. историком и правоведом А.Н. Поповым работа «Диплома-

тическая тайнопись времен царя Алексея Михайловича с дополнением к ней». Обострение проблемы сохранения в тайне содержания текстов обоснованно связывалось автором с интенсификацией сношений Московской Руси с иностранными государствами. Требовалось сохранить в тайне посольскую переписку (*Попов*, 1853, с. 157). Во второй половине XIX в. шифровальные службы в России создаются в Военном министерстве, МИДе и Департаменте полиции МВД. Сфера использования криптографии существенно расширялась: к шифрованию стала прибегать жандармерия [*Ларин*, 2011, с. 25].

Опыт извлечения сведений из письменных коммуникаций внутренних и внешних противников является достаточно актуальной темой для современной отечественной исторической науки. Особую значимость это направление работы специальных служб имеет в пределах транспортной инфраструктуры. Дезорганизация ее работы влечет снижение обороноспособности и разрушение цепочек взаимодействия субъектов экономики.

Развитие железнодорожного транспорта стало основой для охватившей Европу и Северную Америку в XIX в. «транспортной революции». На «чугунке» концентрировалась значительная масса материальных ценностей. Потоки пассажиров и железнодорожные служащие образовывали уникальный социум, в котором переплетались множественные контакты, коммерческие и государственные интересы. В России достаточно быстро пришло осознание необходимости учреждения транспортной полиции. Во время строительства Николаевской железной дороги, соединившей Санкт-Петербург и Москву, в 1844 г. было учреждено первое железнодорожное полицейское управление (О сокращении штата..., 1856). Полицейские функции на железных дорогах выполнялись жандармами. В 1866 г. железнодорожная полиция была исключена из подчинения Министерства путей сообщения и перешла в ведение Корпуса жандармов (Об обязанностях и подчинении..., 1867). Чины жандармских полицейских управлений железных дорог (ЖПУЖД) выполняли функции как общей (охрана порядка), так и политической полиции. Накануне Первой мировой войны им в обязанность также было вменено противодействие шпионажу на вверенных участках, осуществлявшееся во взаимодействии с контрразведывательными отделениями военного ведомства и губернскими жандармскими управлениями (ГАРФ. Ф. 126. Оп. 1. Д. 2. Л. 42–43 об.).

Не только грузы и обыватели перемещались по железным дорогам империи: по ним к своим целям следовали письма политических радикалов и шпионские донесения. Борьба с революционерами и вражескими агентами требовала от жандармов понимания методов обнаружения замаскированных посланий и подходов к осуществлению дешифровки тайнописи.

Комплекс источников, охваченный рамками представленного исследования, состоит из групп документов: адресованные начальникам ЖПУЖД циркуляры Департамента полиции МВД и Отдельного корпуса жандармов о результатах анализа маскировки ведения переписки и ее шифрования шпионами и революционерами; условные алфавиты и перечни условных слов, использовавшиеся военным противником и радикалами для преобразования текстов и защиты от «снятия» их содержимого; делопроизводственная переписка ЖПУЖД и заведующих передвижением войск и военных грузов о неразглашении сведений относительно железнодорожных перевозок в годы Первой мировой войны.

Тайнопись революционного движения на железных дорогах

Низкая оплата и тяжесть труда рабочих и служащих создавали благодатные условия для распространения революционных идей на железных дорогах Российской империи. В период Первой революции в России началось объединение железнодорожных рабочих по линии создания профессионального движения. 20 мая 1905 г. в Москве состоялся I съезд Всероссийского союза железнодорожных рабочих и служащих. Создание союза инициировали революционные партии, отдельные его группы в 1905–1907 гг. готовили вооруженное восстание, проводили забастовки на железных дорогах [*Медведев*, 2018, с. 15]. Выбор пути антиправительственной деятельности требовал от железнодорожников принятия мер к сохранению своих намерений в тайне. В последней четверти XIX – начале XX в. в революционной среде широкое распространение получила переписка, содержащая фрагменты зашифрованного текста. Данное явление

объясняется как подъемом революционного движения, так и ответным усилением контроля политической полиции за деятельностью политически неблагонадежных лиц [*Пылаева,* 2014, с. 22]. При последовавших после убийства императора Александра II террористами «Народной воли» арестах 1881–1882 гг. в руки полиции попало немало шифрованных писем народовольцев [*Гольев* и др., 2006, с. 89]. Показательным является то, что брошюра эсдека В.П. Махновца «О шифрах», опубликованная им в 1902 г. под псевдонимом Бахарев начиналась словами: «Беда, если революционер не умеет записать понятным только ему одному способом секретный адрес или свои соображения – на память не все запомнишь, а записанное обыкновенным способом, того гляди, будет отнято жандармами при обыске и поведет к арестам товарищей и разрушит, может быть целую организацию» (*Бахарев,* 1902, с. 1). На этапе подъема революции (январь – октябрь 1905 г.) интенсивность переписки была для социал-демократов одним из ключевых индикаторов эффективности политической деятельности. После Манифеста 17 октября почти все партийные деятели вернулись из эмиграции, объемы переписки сократились, но своего значения в отношении координации деятельности политических организаций она не утратила [*Беседина, Буркова,* 2021, с. 123].

Противоправные намерения, излагавшиеся в переписке членами Всероссийского союза железнодорожных рабочих и служащих и сочувствующими ему, нередко шифровались для предупреждения их раскрытия царской полицией. Так, 27 июня 1908 г. особый отдел Департамента полиции, осуществлявший криптоаналитическую деятельность[1], т.е. разбор шифров, направил начальникам ЖПУЖД разбор тайнописи, применявшейся железнодорожным союзом. Ключ к шифру был получен агентурным путем: передан внедренным в организацию осведомителем или обнаружен при обыске, произведенном по полученным от внедренного секретного сотрудника сведениям. Начальникам ЖПУЖД надлежало ознакомиться с ним для «соображений при розыске». Перед ними открывалась возможность оперативно принимать должные меры в случае перехвата письма, содержание которого было скрыто представленным ниже шифром (рис. 1).

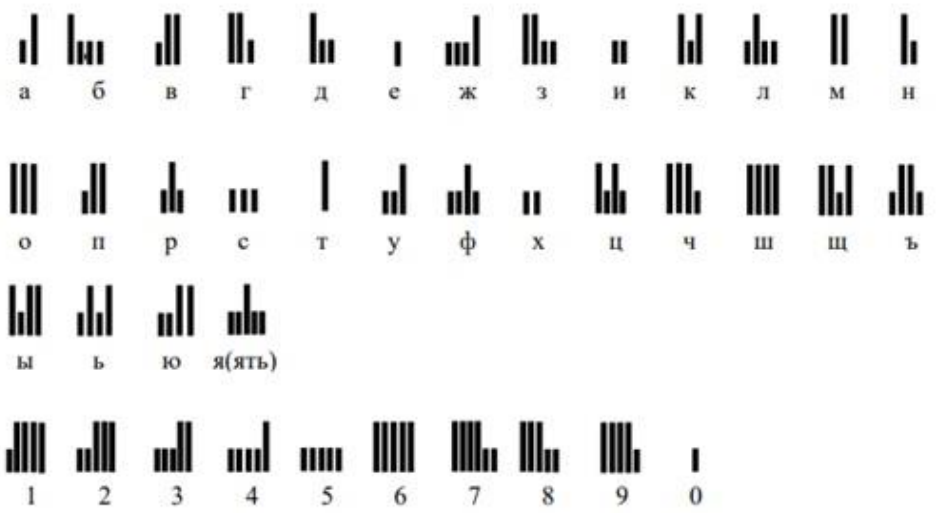

Рис. 1. Шифр, использовавшийся членами железнодорожного союза

В качестве ключа была принята обыкновенная телеграфная азбука с тем лишь отличием, что вместо точки изображалась малая вертикальная линия, а вместо тире – большая (рис. 2).

Рис. 2. Пример зашифрованного предложения, изложенный в циркуляре Департамента полиции МВД

Зашифрованные предложения представляли собой последовательности таких линий (ГАРФ. Ф. 59. Оп. 1. Д. 441. Л. 17).

Использование телеграфной азбуки в качестве шифровального ключа, очевидно, было удобно для служащих железнодорожных телеграфов. Однако такой шифр не обеспечивал должного уровня надежности. В случае перехвата письма владевшему азбукой Морзе человеку достаточно было бы внимательного взгляда на ряды линий двух размеров для того, чтобы увидеть в них знакомые комбинации длинных и коротких сигналов.

В представленной тайнописи каждой букве соответствует одна совокупность символов. Такая система преобразования исходного текста называется шифром простой замены.

Еще один пример использования шифра простой замены раскрывается в сведениях, изложенных в служебной переписке железнодорожных жандармов о деятельности одной из боевых организаций эсеров. В 1908 г. в Москве сложилась группа экспроприаторов. Для организации ограблений артельщиков и почтовых вагонов группа активно вербовала в свои ряды железнодорожных служащих. Ее членами являлись телеграфисты станций Михнево и Кашира по фамилиям Немолодышев и Сушков, помощник начальника станции Домодедово – Картинцев, осуществлявшие перевозку грузов таксировщики и бухгалтер Гончаров со станции Суслово, а также машинист депо Кашира Сиротин. Приобретение эсерами сторонников среди железнодорожных служащих открывало для них возможности получать информацию о передвижениях ценных грузов по «чугунке» и с ее учетом планировать ограбления. Кроме того, находили применение и рабочие навыки железнодорожников. Так, упомянутый телеграфист Немолодышев как бывший слесарь имел токарные станки, на которых он из цинка и меди вытачивал детали запалов бомб. Готовые смертоносные изделия, предназначавшиеся для отправки, Немолодышев хранил закопанными на огороде. Снабжением участников грабежей подложными паспортами занимался Картинцев, который доставал их через бывшего телеграфиста Зубанова, уволенного со станции Белев за участие в отбитии у полиции арестованных во время Декабрьского восстания 1905 г. Процесс планирования и подготовки ограбления на железной дороге был достаточно сложным мероприятием, требовавшим интенсивных коммуникаций между членами преступной группы. Описанная выше боевая организация эсеров пользовалась имевшимся у отдельных ее членов доступом к телеграфу. Для переговоров телеграфисты-революционеры имели свой шифр: А-96, Б-93, В-88, Г-82, Д-76, Е-73, И-65, К-68, Л-56, М-54, Н-50, О-47, П-46, Р-43, С-39, Т-38, У-35, Ф-32, Х-29, Ц-22, Я-11. Кроме того, в начале сеанса связи вызывавший телеграфист должен был подтвердить свою принадлежность к боевой организации и удостовериться в том, что его собеседник также является одним из ее членов. Для этих целей использовались пароли и отзывы. Так, например, при выходе на связь со станцией Кашира телеграфист направлял пароль «3» и ожидал ответ «11». Передавать шифрованную информацию дозволялось только после получения отзыва (ГАРФ. Ф. 59. Оп. 1. Д. 19. Л. 19–20 об.).

Представленный шифр не содержал изъяна, свойственного тайнописи членов железнодорожного союза. Буквам присваивались числовые значения, выбор которых не был определен какой-либо логикой. Вместе с этим нельзя признать и этот шифр в достаточной мере надежным. Его «вскрытие» представляет собой несложный процесс при условии, если лицо, осуществляющее дешифровку, имеет закодированный текст в объеме, достаточном для его рассмотрения с точки зрения статистического анализа. Выявление наиболее часто повторяющихся значений позволяло выдвигать гипотезы о кодировании ими гласных букв, осуществлять подбор их соответствий числовым значениям, исходя из наличия устойчивых комбинаций. Такая тактика дешифровки была проработана и изложена еще в 1466 г. в книге «Трактат о шифрах» итальянского ученого Леона Альберти, в которой он изложил свои наблюдения количественных закономерностей в соотношениях гласных и согласных букв в текстах, а также в их сочетаниях [*Кан,* 2000, с. 39–40].

Чрезвычайно сложными для дешифровки являлись письма, содержание которых преобразовывалось с помощью «книг-ключей». Группа революционеров определяла издание, которое использовала для шифрования сообщений, и каждой букве присваивалось значение «Номер страницы. Номер строки. Порядковый номер буквы в строке». Так, набор 75.2.4 означал, что

нужную букву необходимо было искать на 75-й странице, четвертую во второй строке. Чтобы обнаружить такое издание при обыске полицейские обращали внимание на книги с пометками на страницах, загрязненные от употребления более других [*Гольев* и др., 2008, с. 90].

Уже упомянутая система паролей и отзывов имела достаточно широкое распространение в коммуникациях революционеров. Так, например, 31 января 1908 г. особый отдел Департамента полиции МВД секретным циркуляром за № 123850 уведомил начальников ЖПУЖД о том, что «для более удобной передачи конспиративных сведений» киевской группой анархистов-коммунистов установлены пароли двух родов. Первый пароль выдавался только наиболее доверенным организаторам групп. Лицо, являвшееся с таким паролем, принималось как заслуживающее полного доверия. Пароль звучал следующим образом: «Насильники пируют, помешаем же их пиршеству». Ответ: «Так сомкнем же ряды». Второй пароль «Пришел и ушел, сел и встал», хотя и являлся также конспиративным, но выдавался всем членам группы. Письма, отправлявшиеся ими, полагалось начинать фразой «Серые тучи нависли, теперь опять прояснилось». Такое предложение служило индикатором того, что автором письма действительно является лицо, состоявшее в организации (ГАРФ. Ф. 59. Оп. 1. Д. 446А. Л. 1). В целом подмена смысловых единиц условными понятиями была приемом активно эксплуатировавшимся революционерами. Такие замены, как «блины» вместо «прокламации» и «заболел» вместо «арестован», настолько прочно вошли в обиход, что даже, по признанию самих представителей революционных партий, становились общеизвестными и оказывались негодными для выполнения своего предназначения (*Розенталь*, 1904, с. 14).

Противозаконный характер переписки требовал от революционеров не только сокрытия содержания текстов, но и обеспечения надежности перемещения писем. Выполнению этой задачи также способствовало вовлечение в революционные организации железнодорожников. Жандармская переписка содержит сведения об использовании членами боевых организаций эсеров услуг контроллеров, которые вкладывали шифровки в пакеты со служебными документами (ГАРФ. Ф. 59. Оп. 1. Д. 19. Л. 19–20 об.). Имели место случаи, когда тайнописные тексты пересылались с помощью голубей. В связи с этим внимание железнодорожной полиции было ориентировано на перевозивших этих птиц пассажиров (ГАРФ. Ф. 127. Оп. 1. Д. 37. Л. 29–30).

Защита сведений о перевозках и криптоанализ шифровок противника в годы Первой мировой войны

К началу Первой мировой войны значимость криптографии в достижении преимущества перед противником была бесспорной для политического и военного руководства европейских держав. Получение шифров противника являлось важной целью разведок стран Антанты и центральных держав. Обладание ими создавало возможности для раскрытия планов врага и превентивного реагирования на его намерения. Криптоанализ стал одним из главных орудий войны. Быстровозводимые радиопеленгаторные станции в огромном количестве перехватывали сообщения, при почтовых отделениях работали «черные кабинеты», где осуществлялся перехват вызывавших подозрение отправлений. Даже водолазным отрядам была отведена роль в этой борьбе: они подключались для розыска шифрокниг [*Визавитин* и др., 2017, с. 446]. Первые опыты по перехвату иностранных радиограмм были проведены моряками Балтийского флота летом 1902 г. под руководством изобретателя радио А.С. Попова. Спустя год началось регулярное ведение радиоразведки, осуществлявшейся в условиях резкого расширения объемов зашифрованных передач [*Ларин*, 2014. с. 36–37]. Успехи в создании телеграфа, счетных и пишущих машин, кассовых аппаратов в начале XX в. инициировали интерес к изобретению автоматических машин для шифрования текстовых сообщений [*Бутырский* и др., 2007, с. 88].

В условиях противостояния с Тройственным союзом стабильность функционирования железнодорожного транспорта была критически важным фактором для обеспечения перевозок живой силы, вооружения и снабжения. Немецкие, австрийские и турецкие агенты были заинтересованы в установлении маршрутов прохождения составов с наиболее ценными для русской армии грузов. Требовалось всеми возможными способами нивелировать возможности для перехвата врагом такого рода сведений. Эту цель возможно было достичь ограничением круга

осведомленных о перевозках лиц, а также исключением из передававшихся сообщений прямых упоминаний о наименованиях грузов.

В начале войны железнодорожными жандармами применялась простая кодировка, в соответствии с которой взрывчатые грузы обозначались в телеграммах как «особые воинские», а все прочие – «воинские грузы» (ГАРФ. Ф. 59. Оп. 1. Д. 498. Л. 56). Очевидно, что подобный подход не мог обеспечить надлежащей защиты сведений о перевозках вооружения и снабжения, во-первых, вследствие того, что их отношение к армии было сохранено в наименованиях, а, во-вторых, определение отличия «особых воинских» от «воинских» грузов не могло занять значительного времени для противника. Необходимо было усложнять систему кодирования, исключать из наименований логическую привязку к предназначению и содержанию грузов.

9 августа 1915 г. заведующий передвижением войск и военных грузов по железным дорогам и водным путям Московско-Смоленского района направил в адрес начальников ЖПУЖД перечень обозначений наименований грузов для использования в телеграммах: снаряды, снаряженные ручные гранаты и артиллерийские патроны – «Бук»; винтовочные патроны – «Вол»; взрывчатые вещества и заряды – «Гар»; прочий артиллерийский груз (гильзы, капсюли, втулки, трубки всякого рода, взрыватели, запалы, бикфордов шнур, боевые и светящиеся ракеты, пули и прочее) – «Дом»; орудия – «Зур»; пулеметы – «Коб»; винтовки – «Лак» (ГАРФ. Ф. 59. Оп. 1. Д. 663. Л. 4).

Для обозначения перевозившихся в вагонах грузов, когда это не было очевидно через поверхностное наблюдение, вражеская агентура прибегала к нанесению условных меток на вагоны. Такого рода знаки могли иметь скрытый смысл, который необходимо было донести до находившегося на пути следования состава лица. Были случаи, когда на вагоны с нижними чинами мелом наносились надписи «Следуют консервы», «Следует в Германию партия консервированного мяса», в связи с чем военное руководство обращало внимание железнодорожной жандармерии на необходимость их быстрого устранения в связи с тем, что «не говоря о моральном действии вышеуказанных надписей на нижних чинов, известно, когда подобным образом передавались сведения шпионского характера» (ГАРФ. Ф. 76. Оп. 1. Д. 212. Л. 100).

В ходе переписки противник также применял системы условных обозначений смысловых единиц, содержание которых необходимо было скрыть от русской контрразведки. Так, в декабре 1915 г. железнодорожными жандармами на станции Вильно в вагоне пассажирского поезда были обнаружены забытые неустановленным лицом рукописи и чертежи. В ходе изучения документов был сделан однозначный вывод об их принадлежности вражескому шпиону. При рассмотрении карт было установлено, что города на них не именовались своими названиями, а для каждого существовало свое условное слово: Аварро – Минск; Авур – Столбцы; Альман – Кенигсберг; Амерополис – Полоцк; Анктиф – Ковно и т.д. (ГАРФ. Ф. 59. Оп. 1. Д. 699. Л. 6 об.).

Системами, в которых одной шифруемой смысловой единице присваивалось единственное значение, активно пользовались германцы и австрийцы. Одна из таких систем для непосвященного лица представляла собой шахматную игру по переписке, где каждой координате поля шахматной доски соответствовала скрытая бука, слог или слово. Подозрение такая игра могла бы вызвать у знакомого с шахматами лица, которое, расставив фигуры на доске, попыталось бы ее воспроизвести и обнаружило, что фигуры перемещаются против правил, и в целом движение на игровом поле лишено всякого смысла.

Еще одним подходом к маскированию истинного смысла передававшегося сообщения было придание ему вида коммерческого послания через замену слов понятиями из предпринимательского обихода.

Применялась схожая с рассмотренными выше шифрами революционеров тайнопись, строившаяся на присвоении букве цифровой комбинации. Например, 28 мая 1916 г. Департамент полиции МВД направил начальникам полиции ключ от шифра использовавшегося отдельным немецкими и австрийскими агентами: A–0; B–1; C–2; D–3; E–4; F–5; G–6; H–7; I–8; J–9; K–30; L–47; M–60; N–69; O–77; P–84; Q–90; R–95; S–00; T–04; U–07; V–11; Y–14; Z–17 (ГАРФ. Ф. 76. Оп. 1. Д. 35. Л. 31–32). Ненадежность такого рода шифров при наличии достаточного объема текстов для изучения с позиций статистического анализа уже раскрывалась в

данной статье. Относительно представленного шифра необходимо отметить, что его создатель к тому же облегчил задачу дешифровщику, присвоив буквам с A по J в качестве значений номера по порядку.

Для повышения надежности тайнописи требовалось, чтобы каждой шифруемой единице соответствовало бы не одно, а несколько значений.

Пример такого подхода содержит письмо начальника штаба Отдельного корпуса жандармов от 18 августа 1914 г. за № 1185, в котором сообщалось, что командированные в Россию агенты австрийского Эвиденцбюро при передаче собранных сведений телеграммами условного содержания должны были заменять слово «кавалерия» любым именем, начинающимся на букву К; слово «лошади» – на Л; «артиллерия» – на А, «материал» – на М, выражение «всех родов оружия» – на букву Г. Отметим, что и в этом случае шифровальщик оставлял своему оппоненту, стремившемуся разобраться с содержанием послания, шанс логически его домыслить, восприняв логику шифрования по первым буквам. Эта австрийская тайнопись содержала также дефиниции, которые шифровались только одним условным значением: «мобилизация производится» – «Мориц болен», «всех родов оружия» – «прибывает от Георга». Сведения о количестве поездов, направленных по представлявшему интерес противника направлению, сообщались фразой «через столько-то часов выезжаю туда-то», где значение времени обозначало число составов (ГАРФ. Ф. 59. Оп. 1. Д. 497. Л. 6).

Противостояние в годы Первой мировой войны специалистов по шифровке и дешифровке дало серьезный импульс развитию криптографии. Сохранение секретов требовало усложнения тайнописи.

Немцы пытались защитить свою переписку с помощью сложных комбинаций, вносившихся в объемные книги, по которым работали шифровальщики. Опасность такого подхода заключалась в возможности попадания этих фолиантов в руки противника. Ни один шифровальщик не мог сохранять в своей памяти столь громоздкие ключи, содержавшиеся в них. Такого рода угроза воплотилась в жизнь: 26 августа 1914 г. в Финском заливе у острова Осмуссаар сел на мель германский легкий крейсер «Магдебург». Русские моряки с крейсеров «Богатырь» и «Паллада» подняли из моря сигнальную книгу крейсера, которая затем была переданы британскому адмиралтейству, что сыграло решающую роль в раскрытии военно-морского кода Германии. Знаменитая «Комната 40», служба криптоанализа британского адмиралтейства, началась именно с изучения этой добычи [*Синичeнко*, 2021, с. 20].

Одним из самых известных военных шифров времен столкновения Антанты и Тройственного союза был немецкий ADFGVX, который стал применяться 5 марта 1918 г. в ходе «Битвы Кайзера» – последнего наступления Германии на Западном фронте. Стойкость этого шифра определялась сочетанием замены и перестановки значений [*Сингх*, 2007, с. 122].

Зашифровывание начиналось с заполнения матрицы 6×6, 26 буквами и 10 цифрами в произвольном порядке. Каждая строка и столбец сетки обозначалась одной из букв A, D, F, G, V, X. Как и в шахматной игре координата каждого поля определялась совмещением наименования строки и столбца.

Пример матрицы шифра ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Так, например, на первом этапе шифрования по приведенной выше матрице «9» заменялось на XA, а «h» – на DX. В качестве примера приведем первый этап шифрования сообщения «атака в 10 вечера» (таблица).

Первый этап шифрования по матрице ADFGVX

Сообщение	Attack at 10 pm											
Текст	a	t	t	a	c	k	a	t	1	0	p	m
Шифртекст Шаг 1	DV	DD	DD	DV	FG	FD	DV	DD	AV	XG	AD	GX

Второй этап – перестановка по ключевому слову, которое, как и вид матрицы ADFGVX, должно было быть известным адресату для дешифровки. В верхнюю строку сетки записывались буквы ключевого слова. Под ним в каждую из ячеек матрицы по порядку вписывается одна буква из полученной на первом этапе последовательности. После этого осуществлялась перестановка мест столбцов таким образом, чтобы буквы ключевого слова были размещены по алфавиту. Приведем пример перестановки по ключевому слову MARK (рис. 3).

M	**A**	**R**	**K**		**A**	**K**	**M**	**R**
D	V	D	D		V	D	D	D
D	D	D	V	→	D	V	D	D
F	G	F	D	Перестановка столбцов в соответствии с порядковой позицией букв первой строки в алфавите	G	D	F	F
D	V	D	D		V	D	D	D
A	V	X	G		V	G	A	X
A	D	G	X		D	X	A	G

Рис. 3. Перестановка значений по ключевому слову

После проделанной манипуляции с матрицами шифровальщик последовательно, двигаясь сверху вниз поочередно по каждому столбцу, выписывал буквы. Шифртекст приобретал свой окончательный вид: VDGVVDDVDDGXDDFDAADDFDXG – и передавался с помощью кода Морзе [*Сингх,* 2007, с. 416–417].

Шифр является объектом атаки криптоаналитиков. Как только дешифровщики создают новое средство, обнаруживающее уязвимость шифра, последующее его использование становится бессмысленным. Шифр или выходит из применения, или на его основе разрабатывается новый, более стойкий [*Гребенников,* 2017, с. 10]. Такая судьба ждала и ADFGVX, который с учетом сложности и изящества можно назвать символом критографии Первой мировой войны. По истечению немногим менее четырех месяцем французским криптоаналитикам удалось его вскрыть [*Сингх,* 2007, с. 123].

Маскировка шпионских донесений при транспортировке

Передача телеграмм в военное время была для вражеской агентуры опасным мероприятием вследствие возможности оказаться раскрытым. Тем более что российским правительством был наложен запрет на прием телеграмм от германских и австрийских военнопленных, которые могли согласиться стать соучастниками в передаче сведений, необходимых для вражеского военного руководства (ГАРФ. Ф. 59. Оп. 1. Д. 383. Л. 143). Необходимо обратить внимание не только на особенности тайнописи, к которым прибегал противник, но и на ухищрения, с помощью которых послания покидали пределы Российской империи. Их знание позволяло жандармской железнодорожной полиции перехватывать зашифрованные отправления.

Достаточно распространенным способом пересылки сведений являлось изощренное их размещение в багаже. Железнодорожной полицией вскрывались случаи размещения агентурных донесений, наклеенных на бутылках и ярлыках, прикреплявшихся к чемоданам и сумкам (ГАРФ. Ф. 76. Оп. 1. Д. 35. Л. 31–31 об.). Отмачивались для последующего сокрытия посланий на обороте этикетки от коробков с сардинами. В газетную бумагу, на которую аккуратно наносился текст, заворачивались яблоки, груши и консервные банки. Донесения запекались в хлеб и вкладывались в обертки с шоколадными плитками (ГАРФ. Ф. 59. Оп. 1. Д. 236. Л. 58–58 об.).

Еще одним нестандартным ходом иностранных шпионов было прятание закодированной в условные понятия информацию на самом виду, там, где ее не буду искать, а именно – в газетных объявлениях. В указанное при получении задания на добывание информации издание агент направлял частное или коммерческое объявление, содержавшее условные понятия, характеризовавшие обстановку на железных дорогах (ГАРФ. Ф. 76. Оп. 1. Д. 35. Л. 31–31 об.). Как бы это ни показалось странным, но газетные статьи использовались не только для передачи зашифрованных посланий, но и для разбора тайнописи противника. Австрийцам незадолго до начал Первой мировой войны удалось перехватить шифровку итальянского посла в Константинополе. На основе полученного материала код раскрыть не удалось, и австрийцы реализовали изящную оперативную игру. В одной из италоязычных газет, издававшихся в столице Османской империи, было опубликовано сообщение, имевшее вид утечки информации военного характера. Ознакомившись со статьей, итальянский посол отреагировал как ответственный государственный служащий – передал шифровку с ее содержанием в Рим, не подозревая, что таким образом австрийцы получили ценный материал для криптоанализа, имея на руках исходный текст [*Бабаш, Баранова*, 2020, с. 12].

Наряду с вопросами дешифровки и перехвата донесений агентов противника жандармской полиции и военной контрразведке необходимо было уделять внимание носителю информации. Исследование бумаги с не вызывавшим подозрения текстом бытового характера могло привести к неожиданным результатам. В этом отношении представляют интерес показания вернувшегося из немецкого плена не названного в полицейской служебной переписке чина Русской императорской армии, направленные штабом Отдельного корпуса жандармов для ознакомления в Московское ЖПУЖД. Указанный чин, находясь в неволе, выразил согласие на вербовочный подход, совершенный к нему немецкой разведкой. Приняв предложение выполнять задания по сбору и перевозке секретных сведений в Петрограде, Москве, Твери и Саратове, он, вернувшись в Россию, уведомил об этом военную контрразведку. Так как военнослужащего готовили к выполнению шпионских задач, ему были переданы ценные знания, в том числе относительно способов, к которым германцы прибегали для скрытия добытой информации. Он сообщил, что сведения агенты пересылают под видом обычных писем. На листе бумаги произвольного размера, но достаточной плотности, агент должен был написать обычное письмо химическим карандашом с таким расчетом, чтобы заполнить одну сторону листа и две-три строчки на его обороте. На оставшейся чистой части мягким золотым пером секретными чернилами наносилось представлявшее ценность донесение. В течение 15 минут написанное просушивалось, а затем при помощи ваты смачивалось чаем. После произведенных манипуляций письмо закладывалось в книгу под пресс, чтобы после просушки бумага не деформировалась. При отсылке письмо надлежало складывать таким образом, чтобы написанный секретными чернилами текст был обращен вовнутрь. Для отображения перемещений русских войск использовались открытки: точка, поставленная на верхнем крае карточки, обозначала, что войска двигаются на север, на нижнем – на юг, на левом – на запад, на правом – на восток; в левом верхнем углу – на северо-запад, в правом нижнем – на северо-восток, в нижнем левом – на юго-запад, в правом нижнем – на юго-восток; значительное скопление живой силы отражалось нанесением двух или трех точек (ГАРФ. Ф. 59. Оп. 1. Д. 502. Л. 2–3 об.).

Заключение

Завершая анализ организации жандармской железнодорожной полицией Российской империи служебной деятельности по раскрытию зашифрованных замыслов революционеров, а также донесений вражеских шпионов в годы Первой мировой войны, на основе проанализированной делопроизводственной документации можно сделать вывод о том, что в отношении подбора методов для вскрытия шифров железнодорожные жандармы в значительной степени были зависимы от Особого отдела Департамента полиции МВД, одним из направлений деятельности которого был криптоанализ, а также от специалистов Военного министерства. Ключи поступали в ЖПУЖД в секретных и совершенно секретных циркулярах. Таким образом, железнодорожные жандармы наделялись возможностью вскрывать противозаконные намерения в

пределах вверенных участков «чугунки» и оперативно на них реагировать, не вступая в длительные сношения. Вместе с этим выполнявшие полицейские функции на железных дорогах жандармы аккумулировали уникальный опыт раскрытия ухищрений перевозки секретов, сами становясь источника ценной для защиты отечества информации.

Автоматические машины для шифрования текстов в рассмотренный период еще не стали распространенным инструментом криптографии. Сторонники революции и иностранные шпионы не получили широкой возможности использовать это достижение прогресса против интересов правительства Российской империи. К тому же, перед ними часто стояла задача осуществить зашифровать текст и передать его максимально быстро. Эти обстоятельства определяли распространенность достаточно простых, уязвимых к статистическому анализу шифров простой замены, а также широкое применение перечней условных понятий, которыми подменялись маскировавшиеся смысловые единицы.

Примечания

[1] Криптоанализ (от греч. krypto «тайный» + analysis «разложение, разбор, расчленение») – дешифровка преобразованной в целях сокрытия информации в условиях отсутствия сведений об алгоритме ее шифрования (ключе).

Список источников

Государственный архив Российской Федерации (ГАРФ). Ф. 59. Оп. 1. Д. 19. Л. 19–20 об.; Д. 236. Л. 58–58 об.; Д. 383. Л. 143; Д. 441 Л. 17; Д. 446А. Л. 1; Д. 497. Л. 6; Д. 498. Л. 56; Д. 502. Л. 2–3 об.; Д. 663. Л. 4; Д. 699. Л. 6 об.; Ф. 76. Оп. 1. Д. 35. Л. 31–32; Д. 212. Л. 100; Ф. 126. Оп. 1. Д. 2, Л. 42–43 об.; Ф. 127. Оп. 1. Д. 37. Л. 29–30.

Бахарев В. О шифрах. Женева: Тип. Союза Geneve, route de la Cluse, 7, 1902. 24 с.

Об обязанностях и подчинении Жандармских Полицейских Управлений железных дорог // Полное собрание законов Российской империи, с 1825 г. СПб., 1868. Т. XXXXI. Ч. 2, 8 января 1867, № 44071.

О сокращении штата Полицейского Управления Николаевской железной дороги // Полное собрание законов Российской империи, с 1825 г. СПб., 1857. Т. XXXI. Ч. 1, 12 января 1856, № 30046.

Попов А.Н. Дипломатическая тайнопись времен царя Алексея Михайловича. СПб., 1853. 7 с.

Розенталь П.И. Шифрованное письмо: критика употребляемых у нас систем шифра. Женева: Всеобщий еврейский рабочий союз в Литве, Польше и России (Бунд), 1904. 112 с.

Библиографический список

Бабаш А.В., Баранова Е.К. Криптографические методы обеспечения информационной безопасности до Первой мировой войны // Технологии техносферной безопасности. 2020. № 6(34). С. 12.

Беседина Е.А., Буркова Т.В. «Письмо получено, пишите своим ключом...»: российская социал-демократия против практики перлюстрации в 1905–1907 гг. // Кубанские исторические чтения: материалы XII Междунар. науч.-практ. конф. Барнаул, 2021. С. 122–130.

Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции в первой половине XX в. // Защита информации. INSIDE. 2007. № 4. С. 88–96.

Визавитин О.И., Варламова В.В., Таякин С.Д. Применение криптографии в период Первой мировой войны // Молодой ученый. 2017. № 12(146). С. 445–449.

Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографическая деятельность революционеров в России. 1881–1887 годы: агония «Народной воли» // Защита информации. INSIDE. 2006. № 2. С. 88–96.

Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографическая деятельность революционеров в России. Полиция против революционеров // Защита информации. INSIDE. 2008. № 2. С. 86–96.

Гребенников В.В. Криптология и секретная связь. Сделано в СССР. М.: Алгоритм, 2017. 480 с.

Кан Д. Взломщики кодов. М.: Центрполиграф, 2000. 473 с.

Ларин Д.А. Криптографическая служба МИД Российской империи в период Первой мировой войны // Право и управление. XXI век. 2014. № 3(32). С. 36–41.

Ларин Д.А. Этапы криптографической деятельности в России // Вестник РГГУ. Документоведение и архивоведение. Информатика. Защита информации и информационной безопасности. 2011. № 13(75). С. 11–37.
Медведев С.В. Всероссийский железнодорожный союз в 1907 году по материалам Департамента полиции // История и перспективы развития транспорта на севере России. 2018. № 1. С. 15–18.
Пылаева Е.И. Криптоаналитическая деятельность особого отдела Департамента полиции МВД в начале XX в. (по материалам Вологодской губернии) // Вестник Моск. ун-та. История. 2014. № 3. С. 20–36.
Сингх С. Книга шифров: тайная история шифров и их расшифровки. М.: Астрель, 2007. 447 с.
Синиченко В.В. Перехват донесений специальными службами в годы Первой мировой войны // Исторические чтения на Лубянке. История отечественных спецслужб: источниковедение и историография: материалы XXV Междунар. науч. конф. 2021. С. 19–24.
Соболева Т.А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002. 511 с.

Дата поступления рукописи в редакцию 27.08.2023

CRYPTOGRAPHY ON THE STEEL HIGHWAYS: INTERCEPTION OF REPORTS, DECRYPTION AND PROTECTION OF INFORMATION IN THE ACTIVITIES OF RAILWAY GENDARMES

P. A. Kolpakov

Peoples' Friendship University of Russia, Miklukho-Maklaya str., 6, 117198, Moscow, Russia
1kolpakov1@rambler.ru
ResearcherID: JGY-1738-2023
Scopus Author ID: 58657619800
SPIN: 1054-5704

The article examines the activities of the gendarmerie railway police in the Russian Empire during the period from the last decade of the 19th century to the February Revolution, focusing on their efforts to intercept anti-government correspondence and enemy reports, decrypt them, and protect information about the transportation of military goods. The author uses extensive previously unpublished records from the gendarmerie police departments of the railways to analyze examples of secret writing (cryptograms) used by revolutionaries. The disadvantages of the ciphers used include a logical connection between letters in the source text and positions in conditional alphabets, as well as a specific arrangement of letters that ensures that only one position of the conditional alphabet can correspond to each encrypted value. Militant groups of political radicals actively tried to recruit railway employees, especially telegraph operators, to cooperate in order to receive and transmit information about the passage of trains with valuable cargo. This information was crucial for planning and implementing expropriation actions. During the First World War, the critical importance of communication increased the importance of cryptography and cryptanalysis. To encrypt messages about the state of Russian railways, the enemy used an extensive arsenal of techniques, such as replacing keywords in texts by established methods; using cipherbooks containing various code combinations, and a combination of values replacement and rearrangement according to the developed matrices. The war gave an impetus to the development of cryptography, as ciphers became more complicated for cryptanalysts to decipher. The concealment of the contents of spy reports was ensured not only through the transformation of texts but also through sophisticated methods of packaging information carriers in luggage, among food products, and the use of special ink. In charge of decryption, the railway gendarmes largely depended on the special department of the Police Department of the Ministry of Internal Affairs and the Ministry of War. These agencies provided the necessary keys. In turn, the railway gendarmerie gained valuable experience in intercepting letters containing secrets when they were transported by rail.

Key words: Railway gendarmerie, cryptography, cipher, encryption, decryption, cryptography, cryptanalysis, the Russian Empire, the First World War.

References

Babash, A.V. & E.K. Baranova (2020), "Cryptographic methods of ensuring information security before the First World War", *Tehnologii tehnosfernoy bezopasnosti*, № 6(34), p. 12.
Besedina, E.A. & T.V. Burkova (2021), "The letter has been received, write with your key...: Russian Social Democracy against the practice of perlustration in 1905–1907", in *Kubanskie istoricheskie chteniya. Materialy*

XII Mezhdunarodnoy nauchno-prakticheskoy konferentsii [Kuban Historical Readings. Materials of the 12th International Scientific and Practical Conference], IP Kolmogorov I.A., Barnaul, Russia, pp. 122–130.
Butyrsky, L.S., Golev, Yu.I., Larin, D.A., Nikonov, N.V. & G.P. Shankin (2007), "Cryptographic activities in Sweden in the first half of the 20th century", *Zashhita informatsii. INSIDE*, № 4, pp. 88–96.
Golev, Yu.I., Larin, D.A. & G.P. Shankin (2006), "Cryptographic activities of revolutionaries in Russia. 1881–1887: the agony of «Narodnaya Volya»", *Zashhita informatsii. INSIDE*, № 2, pp. 88–96.
Golev, Yu.I., Larin, D.A. & G.P. Shankin (2008), "Cryptographic activities of revolutionaries in Russia. Police against revolutionaries", *Zashhita informatsii. INSIDE*, № 2, pp. 86–96.
Grebennikov, V.V. (2017), *Kriptologiya i sekretnaya svyaz'. Sdelano v SSSR* [Cryptology and secret communication. Made in the USSR], Algoritm, Moscow, Russia, 480 p.
Kan, D. (2000), *Vzlomshhiki kodov* [Codebreakers], Tsentrpoligraf, Moscow, Russia, 473 p.
Larin, D.A. (2011), "Stages of cryptographic activities in Russia", *Vestnik RGGU. Seriya: Dokumentovedenie i Arhivovedenie. Informatika. Zashhita informatsii i informatsionnoy bezopasnosti*, № 13(75), pp. 11–37.
Larin, D.A. (2014), "Cryptographic service of the Ministry of Foreign Affairs of the Russian Empire during the First World War", *Pravo i upravlenie XXI vek,* № 3(32), pp. 36–41.
Medvedev, S.V. (2018), "All-Russian Railway Union in 1907 according to the materials of the Police Department", *Istoriya i perspektivy razvitiya transporta na severe Rossii,* № 1, pp. 15–18.
Pylaeva, E.I. (2014), "Cryptanalytic activities of the special department of the Police Department of the Ministry of Internal Affairs in the early 20th century (based on the materials of the Vologda province*)", Vestnik Moskovskogo universiteta. Seriya 8. Istoriya,* № 3, pp. 20–36.
Singh, S. (2007), *Kniga shifrov: taynaya istoriya shifrov i ih rasshifrovki* [The Book of ciphers: the secret history of ciphers and their decryption], Astrel, Moscow, Russia, 447 p.
Sinichenko, V.V. (2021), "Interception of reports by special services during the First World War", in *Istoricheskie chteniya na Lubyanke. Istoriya otechestvennyh specsluzhb: istochnikovedenie i istoriografiya. Materialy XXV mezhdunarodnoy nauchnoy konferentsii* [Historical readings on the Lubyanka. The history of Russian special services: source studies and historiography. Materials of the 25th International Scientific Conference], Frontkniga, Moscow, Russia, pp. 19–24.
Soboleva, T.A. (2002), *Istoriya shifroval'nogo dela v Rossii* [The history of encryption in Russia], OLMA-PRESS-Obrazovanie, Moscow, Russia, 511 p.
Vizavitin, O.I., Varlamova, V.V. & S.D. Tayakin (2017), "The use of cryptography during the First World War", *Molodoy uchenyy*, № 12(146), pp. 445-449.