УДК 94 (47) DOI: 10.14529/ssh220203

ОРГАНИЗАЦИЯ ШИФРОВАННОЙ СВЯЗИ В ПОГРАНИЧНЫХ ОКРУГАХ НКВД ДАЛЬНЕГО ВОСТОКА НА НАЧАЛЬНОМ ЭТАПЕ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Н. В. Коршунова, Д. А. Литвинов

Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Российская Федерация

В статье рассматриваются вопросы организации шифрсвязи накануне и в первые месяцы Великой Отечественной войны на Дальнем Востоке. Для того чтобы передача информации была недоступна противнику, необходимо применять ее шифрование или криптографию. Во многом именно качество и скорость передачи зашифрованной информации были залогом успеха проведения различных военных операций.

На основании общей оценки шифрования или криптографии проанализирован механизм обеспечения и организации шифрованной связью пограничных округов Дальнего Востока накануне войны. Отмечено, что смена шифров прямо перед войной, сложность в расшифровке, отсутствие необходимых шифровальных таблиц и блокнотов привели к тому, что в начале войны пограничные войска на Дальнем Востоке оказались фактически без связи. В доказательство указанных тезисов приводятся донесения начальников управления пограничных войск Хабаровского и Приморского округов, в которых указывается на сложность и длительность расшифровки донесений. Отмечена специфика Дальнего Востока и технические способности 40-х гг. XX в. в той части, что времени для доставки документов требовалось намного больше, чем на западной границе.

Анализ недавно рассекреченных шифрограмм из Центрального Архива ФСБ показывает, что организация шифрованной связи как один из составляющих элементов системы управления накануне войны не полностью отвечала предъявляемым к ней требованиям. Большую роль здесь играл тот факт, что в войсках было мало обученных шифровальщиков, понимающих сущность процесса шифрования. Для этого требовалось хорошее знание математики, которым среди связистов пограничных войск мало кто владел в должной мере. Сложности с дешифровкой приводили к тому, что офицеры пренебрегали мерами безопасности, и это приводило в утечке информации, в том числе и «ключей» к шифрам.

Несмотря на то что это была лишь одна из множества сложных задач, которую в оперативном порядке было необходимо решать советскому правительству накануне и в первые месяцы войны, ее нельзя назвать второстепенной. Отсутствие точных указаний, получение дезинформации привели к тому, что и на Дальнем Востоке возникли большие сложности в управлении пограничными войсками. В данном регионе, в отличие от западных границ, это не привело к катастрофическим последствиям, однако существенно затруднило управление войсками на данных территориях. Данная проблема оказалась настолько очевидной, что Верховное командование приложило огромные усилия для обеспечения и налаживания связи в течение всей Великой Отечественной войны.

В заключении обозначена важность грамотного обеспечения шифрсвязи для оперативного управления войсками, особенно накануне и во время Великой Отечественной войны.

Ключевые слова: криптография, пограничные войска, Дальний Восток, организация шифрсвязи накануне Великой Отечественной войны, германская разведка.

Введение

Одним из важнейших вопросов готовности Красной Армии к Великой Отечественной войне является анализ организации связи как средства управления войсками. Для того чтобы передача информации была недоступна противнику, необходимо было применять ее шифрование или криптографию. Уточним, что криптографическая деятельность включает в себя «…не только шифрование и дешифрование, но и организацию каналов передачи сообщений (системы связи), использование различных методов защиты информации (стеганография, физическая защита собственных линий связи и т. д.), организацию перехвата шифрованной информации противника» [1, с. 8]. Во многом именно качество и скорость передачи зашифрованной информации, умение грамотно ее расшифровать были залогом успеха проведения различных оборонительных и военных операций.

Обзор литературы

История криптографии изучалась отдельными учеными, в большей степени математиками и специалистами с техническим образованием с точки зрения самого процесса шифрования информации, анализа эффективности отдельных специальных технологий, конструкции и преимуществ шифровальных машин. Определенный интерес представляют работы, посвященные истории шифровальной техники и шифровальной службе в целом [2–7]. Отдельные вопросы как организации специальной связи, так и роли зашифрованных способов передачи информации в период Великой Отечест-

венной войны представлены в работах Н. Н. Токаревой [8], Т. А. Соболевой [9], В. В. Павлова, В. И.Астрахана, В. Г. Чернеги, Б. Г. Чернявского [10] и других. Здесь авторы рассматривают историю шифрования в целом и в период начала Великой Отечественной войны в частности [10, 11].

В 2015 г. вышло пятнадцатитомное издание «Великая Победа», в котором авторы представляют современный взгляд на историю Второй мировой войны. 10-й том данного издания («Война в эфире») полностью посвящен организации связи на войне, в том числе шифровальной связи [1]. Собственно, шифрсвязи на Дальнем Востоке, но более позднего периода посвящена статья Д. А. Ларина [12].

Учитывая специфику темы, ее секретность, зарубежных исследований, посвященных именно российской шифрсвязи, нет. Однако следует выделить капитальный труд Ф. Бауера, профессора Мюнхенского университета, в котором обстоятельно рассматриваются общие вопросы истории криптографии [13].

Методы исследования

В рамках данной статьи предполагается исследование истории шифрования не с технической точки зрения, а как необходимое условие организации связи накануне и в начале Великой Отечественной войны. Именно поэтому методологической основой подготовки и написания материала явилось использование методов, применяемых в рамках исторической науки. В работе были использованы общенаучные методы историзма, анализа, синтеза и обобщения, а также отдельные математические методы. Были проанализированы донесения командиров пограничных воинских частей, расквартированных на Дальнем Востоке, в которых активно обсуждались проблемы организации связи.

Результаты и дискуссия

Оперативность в передаче информации, донесений и приказов, обеспечение их секретности – необходимое условие грамотного управления, особенно на войне. От скорости доставки и криптографической надежности шифрованных сообщений часто зависел успех в управлении воинскими частями, а в дальнейшем и исход сражений. Опыт прошлых войн показал, что успехи и неудачи боевых действий во многих случаях зависели от состояния связи, а шифрованная связь являлась одним из главных ее элементов и служила для передачи секретной информации. В то же время в СССР система шифрования только зарождалась, что создавало дополнительные сложности ее внедрения в войсках, особенно на Дальнем Востоке с учетом его удаленности от центра страны [9, с. 87].

В пограничных частях Дальнего Востока отсутствовали специальные шифровальные машины, что существенно затрудняло процесс как шифрования, так и расшифровки. Сообщения кодировались вручную с использованием кодовых таблиц, что вызывало очень большие сложности.

Согласно исходящей шифртелеграмме начальника штаба Управления пограничных войск НКВД Хабаровского округа полковника Д. В. Казакевича от 14 июня 1941 года № 2063 [14, Д. 1712, Л. 116], отправленной в Главное управление пограничных войск НКВД, в июне 1941 г. на основании указания № 19/122132/ШО, в пограничных округах происходила смена шифровального кода 17 на 14 и перешифровальных таблиц и блокнотов к нему. Смена кода означала смену цифр. При наличии специальной таблицы это было хотя и сложнее шифровать, чем на машине, но все-таки достаточно оперативно. В противном случае переписка могла занять очень много времени.

Подобный шифр выглядел следующим образом [1, с. 112]:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
01	6	05	72	2	91	3	02	70	1	90	4	03	99	96	5

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
71	75	78	00	04	06	8	07	76	73	74	92	08	09

Из донесения следует, что перешифровальными таблицами и блокнотами с новым кодом 14 обеспечен только сам округ и в соответствии с директивами Главного управления пограничных войск № 19/122024/ШО и 19/122040/ШО контрольно-пропускные пункты Сахалина «Кайган» и «Катангли», имевшие только радиосвязь. Также кодом 14, но без таблиц и блокнотов, обеспечены пограничные отряды, так как округ их из Главного управления пограничных войск не получил. В донесении округ просит дать указание, как в данной ситуации работать с имеющимися документами, особенно с частями, не имеющими проводной линии связи, и запросил, будут ли высланы блокноты для работы с новым кодом 14.

Все документы для шифрования сразу в пограничные войска полностью не поступали, поэтому пограничные округа Дальнего Востока накануне войны не могли, если это потребуется, одномоментно перейти на работу с новыми кодами шифрсвязи со всеми подчиненными подразделениям.

Управления пограничных округов находились на значительном расстоянии от остальных воинских частей, очевидно, что необходимо было большое количество времени для обеспечения доставки зашифрованных документов и их изучения. Противники тоже не дремали: германская разведка завладела шифровальными кодами, таблицами, блокнотами в захваченных подразделениях НКВД и посылала ложные сообщения для нарушения управления. Необходимо было как-то исправлять ситуацию. Следовало менять принципы шифрованной связи.

Данная проблема наиболее рельефно проявилась при организации работы метеорологической службы. В соответствии с шифртелеграммой Отдельной авиабригады пограничных войск НКВД от 22 июня 1941 г. № 34201/1192 командирам всех

авиачастей пограничных войск предписано с 19:00 московского времени 22 июня ввести в действие для кодирования метеосведений код гидрометслужбы «Зенит», таблицу № 28, первый ключ № 349, третий ключ № 77, четвертый ключ № 473». Это означает, что только гидрометслужбы авиачастей пограничных войск были заранее снабжены необходимым количеством кодов, ключей и таблиц к ним в должном количестве для передачи и приема метеоданных [14, Д. 1559, Л. 239].

Уже тогда гидрометеорологическая служба обеспечивала военных данными о текущей и ожидаемой погодной обстановке, степени ее влияния на действия войск, применение оружия и использование технических средств [15, с. 28]. Данная информация широко использовалась при планировании и проведении операций и боев. НКВД СССР обращал внимание особых отделов на необходимость надежного шифрования метеорологических сведений на свободной от противника территории. Они не должны были допустить использования метеоданных противником для своих целей [16, с. 375].

Другим шагом для исправления ситуации на основании шифртелеграммы Отдельной авиабригады Пограничных войск НКВД от 22 июня № 34202/1193 стал приказ немедленно прекратить использование имеющихся кодов авиабригады. Все отправленные и полученные радиограммы обрабатывать через штаб пограничных округов. Радиосвязь с Москвой использовать по мере надобности, для передачи радиограмм пограничного округа [14, Д. 1559, Л. 240].

Все эти меры привели к тому, что все авиачасти пограничных войск НКВД, даже западных округов, не могли работать с имеющимися шифровальными документами (они оказались разными). Кроме того, штабы пограничных округов и авиачастей находились на значительном расстоянии, время получения и отправления шифртелеграмм существенно затягивалось.

Шифры срочно надо было менять. В соответствии с шифртелеграммой Главного управления пограничных войск от 22 июня № 34166/1156 пограничным отрядам было приказано ввести систему паролей к коду РК-2 с книжной перешифровкой. Данное донесение было отправлено начальникам Управлений пограничных войск НКВД в города Читу, Хабаровск, Владивосток, Ташкент, Алма-Ату, Новосибирск и начальнику 4 Архангельского пограничного отряда, то есть туда, где боевых действий не было. Пароли составлялись начальником отряда на каждые сутки, они состояли из восьмизначного числа и выдавались начальникам нижестоящих подразделений систематически в возможно минимальном количестве, с учетом наличия существующих средств и сроков доставки. Паролем перешифровывались показательные группы каждой телеграммы: первыми четырьмя цифрами – первая показательная группа, остальными четырьмя – вторая показательная группа [14, Д. 1559, Л. 195–197]. Менялся и порядок шифрования, который оказался сложным и малопонятным даже для специалистов: «…места показательных групп определяются обусловленными цифрами пароля, например: 2 и 5. Если вторая цифра пароля 5, то первая перешифрованная показательная группа ставится на пятое место от начала и если пятая цифра пароля 3, то вторая показательная группа становится на 3 место…». Настоящее распоряжение необходимо было доставлять в пограничные отряды и подразделения только нарочным. Новый порядок перешифрования указано ввести одновременно во всех частях и подразделениях после получения.

Начальниками пограничных округов были отправлены донесения о сроках доставки в отдаленные пограничные отряды распоряжения Главного управления пограничных войск № 34166/1156, в связи с чем произошла задержка введения указанной системы по всему округу. Так, начальник Управления пограничных войск НКВД Приморского округа в шифртелеграмме от 26 июня № 2465 указал, что для 60 погранотряда (Отдельный Камчатский пограничный отряд) информация получена 15 августа, 61 погранотряда (Отдельный Магаданский пограничный отряд) – 1 августа, 62 погранотряда (Владивостокский пограничный отряд) – 25 июля [14, Д. 1714, Л. 5]. Такая же картина была и в Управлении пограничными войсками НКВД Хабаровского округа [14, Д. 1715, Л. 234]. Донесения Хабаровского и Приморского округов показывают, что время доставки документальных материалов на Дальнем Востоке в летний период составляет минимум 2 месяца, без учета доставки в подчиненные подразделения погранотрядов и изучения документов, проведения дополнительных занятий и инструктажей с личным составом, допущенным к шифровальной работе.

Смена шифров выявила и иные существенные недостатки организации шифрсвязи в целом. Выявлена неготовность пограничных войск НКВД к моментальному переходу к новой системе шифрования информации, т. к. не были заранее переданы в подразделения резервные коды, таблицы и блокноты. Новая система шифрования была передана шифртелеграммой, что само по себе привлекло внимание германской и японской разведок. В пограничные округа не были высланы в необходимом количестве шифровальные документальные материалы (блокноты, таблицы). Новая система шифрования ранее не использовалась, и сотрудники шифровальных отделений ей не обучались. Шифртелеграммы стало просто невозможно прочитать.

Вот несколько примеров. Из донесения Управления пограничных войск НКВД Туркменского округа от 24 июня № 2344 следует: «Сообщаю Вам, что Ваши шифртелеграммы № 1192 показательная группа 4 месте – 34475, если считать за 23 июня

группа 4, ряд 475 такого ряда блокноте № 027 за 23 июня нет. Шифртелеграмма № 1193 показательная группа 33953 ряд есть, но расшифрованию не поддается. Одновременно третий раз сообщаю, радиограмма № 1158 группа 14, 15, 16 расшифрованию не поддается. Шифртелеграмма № 1156 группа 158–159 и в продолжении группы 39, 40 расшифрованию не поддаются и само содержание текста шифртелеграммы адресату не понятно, последнюю прошу повторить» [14, Д. 1713, Л. 153]. То же самое в исходящей шифртелеграмме Управления пограничных войск НКВД Хабаровского округа от 29 июня № 2564, подписной № 321: «четвертый раз просим проверить и повторить 34159 и 34201. Отсутствие ответа задерживает вручение адресату» [14, Д. 1714, Л. 110].

Как видно из приведенных примеров, Хабаровский и Приморский округа вплоть до 29 июня не могли расшифровать шифртелеграммы № 34201 и 34202 от 22 июня 1941 г., которые были адресованы командирам авиачастей и разъясняли порядок шифрования метеосведений и работы в радиосети.

Шифртелеграмма № 34201 (первая из названных) была перенаправлена всем командирам авиачастей за № 34302/1304 от 26 июня, и в ней уже был установлен срок перехода на новый порядок шифрования по коду «Зенит» с 00:00 26 июня 1941 г. (по московскому времени). Интересно только, что шифртелеграмма составлена в 18:45 26 июня, а зашифрована в 22:00 27 июня (по московскому времени) [14, Д. 1559, Л. 346–347]. Когда она была получена в Хабаровске и Владивостоке, можно только предположить, но факт того, что Хабаровск и Владивосток вплоть до 29 июня 1941 г. ее еще не получили, говорит сам за себя.

Большой промежуток времени от зашифрования до получения адресатом говорит о большом количестве исходящих и входящих шифртелеграмм и малочисленности штатов шифровальных отделений НКВД, а также свидетельствует об их неготовности работать в период ведения боевых действий.

Проблема была очевидна, и данные вопросы были подняты в Главном управлении пограничных войск НКВД. Результатом обсуждения данной проблемы стало направление в адрес всех начальников Управлений пограничных войск НКВД 26 июня шифртелеграммы № 34307/1310. В документе говорилось, что в целях сокращения шифрпереписки шифрсвязь следует использовать по мобилизационным и оперативным вопросам, требующим немедленной информации или указания командования Главного управления пограничных войск с отметкой в начале текста: «расшифровать немедленно, а по остальным вопросам использовать другие виды связи. Подписывать шифровки должны только начальники Управлений и их заместители» [14, Д. 1559, Л. 352].

Сразу же после нападения на СССР немцы развернули на территории нашей страны активную разведывательно-диверсионную деятельность. Помимо всего прочего, целью немецко-фашистских операций была дезорганизация советских линий связи для обеспечения собственных военных успехов. В частности, овладение советскими шифрами давало захватчикам широкий простор для возможного проведения мероприятий по дезинформации советских войск. Документы подтверждают, что такие факты имели место.

Так, в шифртелеграмме Главного управления пограничных войск НКВД от 13 июля № 34564 / 14516, отправленной всем начальникам пограничных войск, сказано: «08.07.41 г. командир одного из стрелковых полков, расположенных на границе с Турцией, получил по проводам ЛКС шифровку, в которой Штадив предлагал начать обстрел сопредельной территории. При выяснении оказалось, что Штадив такой шифровки не давал. В целях исключения возможности использования противником наших шифров предлагаю: начальникам погранвойск округов или лицам, их замещающим, составлять пароли из слов на каждые сутки разные. Пароли составляются на минимальный срок, с расчетом доставления их нарочным в погранотряды. При подписи шифровки впереди ее проставляется пароль» [14, Д. 1560, Л. 40]. Очевидно, что исполнение данного приказа сильно бы осложнило обстановку на границе с Турцией.

Оккупанты подбросили ряд подложных шифрограмм, что привело к определенным сложностям в организации приведения войск в боевую готовность на Дальнем Востоке. Так, в шифртелеграмме Главного управления пограничных войск НКВД из Куйбышева от 31 июля № 1001/477, отправленной в соответствующее управление в г. Москве сказано: «передаю текст полученной 30.07.41 г. шифртелеграммы от начальника ОУВС Хабаровска на имя бригинтенданта Воробьева: “По приказу Берия, Кузнецова моротряды, речдивизионы переходят в распоряжение РККФ. Срочно телеграфьте порядок передачи снабжения всеми видами довольствия”. Прошу телеграфировать дан ли такой приказ Хабаровску и Владивостоку» [14, Д. 1561, Л. 6]. Такое указание действительно было отдано, но только 22 июня: согласно шифртелеграмме ГУПВ от 22 июня (зашифрована в 03:20 по московскому времени) № 34157/1151, отправленной только в Архангельск, Мурманск, Ленинград, Таллин, Симферополь, Тбилиси, Кишинев. Начальникам пограничных войск было указано передать морские и речные суда в оперативное подчинение военному совету флота [14, Д. 1559, Л. 190]. Подписано данное указание заместителем народного комиссара внутренних дел СССР генерал-лейтенантом И. И. Масленниковым [1].

В 1941 г. корабли и катера Хабаровского и Приморского округов были переданы в оперативное подчинение Амурской краснознаменной военной флотилии и Тихоокеанского флота МВФ СССР, но это было другое указание и в соответст-

вии с «Инструкцией о порядке перехода морских пограничных частей НКВД в оперативное подчинение военным советам флотов и флотилий МВФ СССР по оперативным готовностям № 1 и № 2» от 27.02.1940 г. И использовались они в первую очередь для выполнения задач по охране границы [14, Л. 17–18]. Таким образом, повторная «ложная» шифрограмма вызвала недоумение командования пограничными войсками и, как следствие, задержку выполнения приказов.

Выводы

Трудно переоценить связь на войне. Здесь играют роль и скорость передачи информации, и ее точность, и грамотно организованная секретность. Руководство страны это понимало. Поэтому перед войной шифровальные машины начали выпускать большими партиями. К сожалению, войска, в том числе пограничные части Дальнего Востока, техникой снабдить не успевали, поэтому приходилось использовать старые способы шифрования, которые были затратными по времени и силам.

Анализ недавно рассекреченных шифрограмм из Центрального Архива ФСБ показывает, что организация шифрованной связи как один из составляющих элементов системы управления накануне войны не полностью отвечала предъявляемым к ней требованиям. Большую роль здесь играл тот факт, что в войсках было мало обученных шифровальщиков, понимающих сущность процесса шифрования. Для этого требовалось хорошее знание математики, которым среди связистов пограничных войск мало кто владел в должной мере. Сложности с дешифровкой приводили к тому, что офицеры пренебрегали мерами безопасности, и это приводило к утечке информации, в том числе и «ключей» к шифрам.

Несмотря на то что это была лишь одна из множества сложных задач, которую в оперативном порядке было необходимо решать советскому правительству накануне и в первые месяцы войны, ее нельзя назвать второстепенной. Не исключено, что именно отсутствие налаженной связи привело к серьезным последствиям на западной границе, особенно в первые дни войны. Отсутствие точных указаний, получение дезинформации привели к тому, что и на Дальнем Востоке возникли большие сложности в управлении пограничными войсками. В данном регионе, в отличие от западных границ, это не привело к катастрофическим последствиям, однако существенно затруднило управление войсками на данных территориях. Данная проблема оказалась настолько очевидной, что Верховное командование приложило огромные усилия для обеспечения и налаживания связи в течение всей Великой Отечественной войны.

Литература

1. Великая Победа : в 15 т. / под общ. ред. С. Е. Нарышкина, А. В. Торкунова. – М. : МГИМО-Университет, 2015. – Т. 10: Война в эфире. – 356 с.

2. Дадуков, Н. С. Советская шифровальная техника: ленинградский период: 1935–1941 / Н. С. Дадуков, Г. А. Репин, М. М. Скачков, Ю. П. Филин // Защита информации. Инсайд. – 2006. – № 5. – С. 75–79.

3. Жуков, В. В. Из истории шифровальной службы России / В. В. Жуков // Вестник Всероссийского института повышения квалификации сотрудников МВД России. – 2006. – № 2 (2). – С. 63–66.

4. Куренков, Г. А. Организация защиты информации в структурах РКП (б) – ВКП (б). 1918–1941 гг. : автореф. дис. ... канд. ист. наук / Г. А. Куренков. – М., 2010. – 28 с.

5. Ларин, Д. А. Советская шифровальная служба в годы Великой Отечественной войны / Д. А. Ларин // Известия Уральского государственного университета. Серия 1 «Проблемы образования, науки, культуры». – 2011. – Т. 86, № 1. – С. 69–80.

6. Пядышева Е. Б. 100 лет шифровальной службе МИД России / Е. Б. Пядышева // Международная жизнь. – 2021. – № 4. – С. 1–45.

7. Солодилов, А. В. Объективные факторы, повлиявшие на состояние и развитие красной армии в предвоенные годы / А. В. Солодилов, В. В. Бруз // Вестник Московского государственного областного университета. Серия «История и политические науки». – 2020. – № 2. – С. 134–144.

8. Токарева Н. Н. Об истории криптографии в России / Н. Н. Токарева // Прикладная дискретная математика. – 2012. – № 4 (18). – С. 82–107.

9. Соболева, Т. А. История шифровального дела / Т. А. Соболева. – М., 2002. – 103 с.

10. Правительственная электросвязь в истории России / В. В. Павлов, В. И. Астрахан, В. Г. Чернега, Б. Г. Чернявский. – М. : Наука, 2001. – Ч. 1 : 1917–1945. – 2001. – 358 с.

11. Бабиевский, В. В. Криптографический фронт Великой Отечественной. Советская шифровальная служба / В. В. Бабиевский, Л. С. Бутырский, Д. А. Ларин, Г. П. Шанкин // Защита информации. Инсайд. – 2010. – № 6 (36). – С. 74–86.

12. Ларин, Д. А. Последний аккорд Второй мировой. Войска правительственной связи в войне с Японией / Д. А. Ларин // Защита информации. Инсайд – 2015. – № 5 (65). – С. 82–96.

13. Бауэр, Ф. Расшифрованные секреты. Методы и принципы криптологии / Ф. Бауэр. – М. : Мир, 2007. – 550 с.

14. Центральный архив ФСБ РФ. Ф. 3. Оп. 8.

15. Нарышкин, С. Н. Великая Победа. Т. VII. Радиофронт / С. Н. Нарышкин, А. В. Торкунов. – М., 2015. – 483 с.

16. Патрушев, Н. П. Органы государственной безопасности СССР в Великой Отечественной войне : сборник документов. Т. 3. Кн. 1. Крушение «Блицкрига». 1 января – 30 июня 1942 г. / Н. П. Патрушев. – М. : Русь, 2003. – 246 с.

Коршунова Надежда Владимировна – доктор исторических наук, доцент, декан исторического факультета, Южно-Уральский государственный гуманитарно-педагогический университет (Челябинск), e-mail: korshunovanv@cspu.ru. ORCID 0000-0002-4648-0893

Литвинов Дмитрий Александрович – аспирант, Южно-Уральский государственный гуманитарно-педагогический университет (Челябинск), e-mail: litvinovdakhabarovsk@mail.ru. ORCID 0000-0002-8613-5592

Поступила в редакцию 8 декабря 2021 г.

DOI: 10.14529/ssh220203

ORGANIZATION OF ENCRYPTED COMMUNICATION IN THE NKVD BORDER DISTRICTS OF THE FAR EAST IN THE INITIAL STAGE OF THE GREAT PATRIOTIC WAR

N. V. Korshunova, D. A. Litvinov

South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russian Federation

The research centers around the organization of encrypted communication on the eve and in the first months of the Great Patriotic War in the Far East. Encryption or cryptography was vital to make information transfer inaccessible to the enemy. In many respects, the quality and speed of transmission of encrypted information ensured the success of various military operations.

The authors analyzed the mechanism of providing and organizing encrypted communication in the Far East border districts on the eve of the war, based on a general assessment of encryption or cryptography. It noted that the change of ciphers just before the war, difficulty in deciphering, absence of necessary cipher tables and encryption pads resulted in an almost complete lack of communication for the border troops in the Far East at the beginning of the war. To support the thesis, the reports of the Border Force Department heads of the Khabarovsk and Primorsk districts are provided, which reveal the complexity and duration of decoding. The specific features of the Far East and the technical capabilities of the 1940s are noted in terms of a bigger amount of time required for document delivery compared to the western borders.

The analysis of recently declassified code cables from the FSB Central Archive shows that the organization of cipher communications, as one of the components of the control system on the eve of the war, did not fully comply with the requirements imposed on it. One of the main causes was a severe shortage of specially trained encryption experts in the troops having in-depth understanding of the essence of the encryption process. All these would call for advanced knowledge of mathematics, which only a few of the wire crew in the border troops had. Difficulties in decryption resulted in information leakage, including the cipher keys, quite often caused by officers who neglected security measures. Although this was only one of the numerous complex tasks that required immediate tackling of the Soviet government on the eve and in the first months of the war, it was not a minor one. The lack of precise instructions and disinformation gained, caused great difficulties in the command and control over the border troops in the Far East as well. In this region, this did not have such a devastating impact as on the western borders, but substantially hampered the command and control over the troops in these territories. This problem was so obvious that the Supreme Command made every effort to ensure and establish communications throughout the Great Patriotic War.

The conclusion stresses the importance of ensuring proper encrypted communications for command and control over the troops, especially on the eve and during the Great Patriotic War.

Keywords: cryptography, border troops, the Far East, organization of encrypted communication on the eve of the Great Patriotic War, German intelligence.

References

1. Velikaya Pobeda [Great Victory]: v 15 t. / pod obshch. red. S.E. Naryshkina, A.V. Torkunova; Mosk. gos. in-t mezhdunar. otnoshenij (un-t) MID Rossii, Centr voenno-politicheskih issledovanij. M.: MGIMO-Universitet, 2015. T. 10: Vojna v efire [War on the Air]. 356 s.

2. Dadukov N.S., Repin G.A., Skachkov M.M., Filin Yu.P. Sovetskaya shifroval'naya tekhnika: leningradskij period: 1935–1941 [Soviet Encryption Technology: Leningrad Period: 1935–1941] // *Zashchita informacii. Insajd*. 2006. № 5. S. 75–79.

3. Zhukov V.V. Iz istorii shifroval'noj sluzhby Rossii [From the History of the Encryption Service of Russia] // *Vestnik Vserossijskogo instituta povysheniya kvalifikacii sotrudnikov MVD Rossii*. 2006. № 2 (2). S. 63–66.

4. Kurenkov G.A. Organizaciya zashchity informacii v strukturah RKP (b) – VKP (b). 1918–1941 gg.: avtoref. dis. ... kand. ist. nauk [Organization of Information Protection in the Structures of the RCP (b) – the CPSU (b). 1918–1941: Abstract of Dissertation of Candidate Historical Sciences]. M., 2010. 28 s.

5. Larin D.A. Sovetskaya shifroval'naya sluzhba v gody Velikoj Otechestvennoj vojny [Soviet Encryption Service during the Great Patriotic War] // *Izvestiya Ural'skogo gosudarstvennogo universiteta: Seriya 1: Problemy obrazovaniya, nauki, kul'tury*. 2011. T. 86, № 1. S. 69–80.

6. Pyadysheva E.B. 100 let shifroval'noj sluzhbe MID Rossii [100 Years of the Russian Foreign Ministry's Encryption Service] // *Mezhdunarodnaya zhizn'*. 2021. № 4. S. 1–45.

7. Solodilov A.V., Bruz V.V. Ob'ektivnye faktory, povliyavshie na sostoyanie i razvitie krasnoj armii v predvoennye gody [Objective Factors that Influenced the State and Development of the Red Army in the Pre-War Years] // *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Istoriya i politicheskie nauki*. 2020. № 2. S. 134–144.

8. Tokareva N.N. Ob istorii kriptografii v Rossii [About the History of Cryptography in Russia] // Prikladnaya diskretnaya matematika. 2012. № 4 (18). S. 82–107.

9. Soboleva T.A. Istoriya Shifroval'nogo dela [The History of the Encryption Business]. M., 2002. 103 s.

10. Pravitel'stvennaya elektrosvyaz' v istorii Rossii [Government Telecommunications in the History of Russia] / V.V. Pavlov, V.I. Astrahan, V.G. CHernega, B.G. CHernyavskij. M.: Nauka, 2001 Ch. 1: 1917–1945. 2001. 358 s.

11. Babievskij V.V., Butyrskij L.S., Larin D.A., Shankin G.P. Kriptograficheskij front Velikoj Otechestvennoj. Sovetskaya shifroval'naya sluzhba [Cryptographic Front of the Great Patriotic War. Soviet Encryption Service] // *Zashchita informacii. Insajd*. 2010. № 6 (36). S. 74–86.

12. Larin D.A. Poslednij akkord Vtoroj mirovoj. Vojska pravitel'stvennoj svyazi v vojne s Yaponiej [The Last Chord of the Second World War. Government Liaison Troops in the War with Japan] // *Zashchita informacii. Insajd*. 2015. № 5 (65). S. 82–96.

13. Bauer F. Rasshifrovannye sekrety. Metody i principy kriptologii [Deciphered Secrets. Methods and Principles of Cryptology]. M.: Mir, 2007. 550 s.

14. Central'nyj arhiv FSB RF. F. 3. Op. 8.

15. Naryshkin S.N., Torkunov A.V. Velikaya Pobeda. T. VII. Radiofront [The Great Victory. Vol. VII. Radiofront.]. M., 2015. 483 s.

16. Patrushev N.P. Organy gosudarstvennoj bezopasnosti SSSR v Velikoj Otechestvennoj vojne: Sbornik dokumentov. T. 3. Kn. 1. Krushenie «Blickriga». 1 yanvarya – 30 iyunya 1942 g. [State Security Bodies of the USSR in the Great Patriotic War: A Collection of Documents. Vol. 3. Book 1. The collapse of the «Blitzkrieg». January 1 – June 30, 1942]. M.: Rus', 2003. 246 s.

Nadezhda V. Korshunova – D. Sc. (History), Associate Professor, Dean of the Faculty of History, South Ural State Humanitarian Pedagogical University (Chelyabinsk), e-mail: korshunovanv@cspu.ru

Dmitry A. Litvinov – Postgraduate Student, South Ural State Humanitarian Pedagogical University (Chelyabinsk), e-mail: litvinovdakhabarovsk@mail.ru

Received December 8, 2021

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Коршунова, Н. В. Организация шифрованной связи в пограничных округах НКВД Дальнего Востока на начальном этапе Великой Отечественной войны / Н. В. Коршунова, Д. А. Литвинов // Вестник ЮУрГУ. Серия «Социально-гуманитарные науки». – 2022. – Т. 22, № 2. – С. 20–26. DOI: 10.14529/ssh220203

FOR CITATION

Korshunova N. V., Litvinov D. A. Organization of Encrypted Communication in the NKVD Border Districts of the Far East in the Initial Stage of the Great Patriotic War. *Bulletin of the South Ural State University. Ser. Social Sciences and the Humanities*, 2022, vol. 22, no. 2, pp. 20–26. (in Russ.). DOI: 10.14529/ssh220203