
Вадим Гребенніков
Радянська криптологія
Гребенніков В.В.
ІСТОРІЯ КРИПТОЛОГІЇ
&
СЕКРЕТНОГО ЗВ'ЯЗКУ
Історія спецзв'язку

Вадим Гребенников

Радянська криптологія

«Издательские решения»

Гребенников В.

Радянська криптологія / В. Гребенников — «Издательские решения»,

ISBN 978-5-4493-0826-9

Книга розповідає про історію народження й розвитку радянської криптології та радіорозвідки, розробки та застосування шифрувальних машин, а також утворення криптологічних служб СРСР та їхню боротьбу у «полюванні» за шифрами супротивника, зокрема, США і НАТО. Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет. Книгу можна знайти на сайті: http://cryptohistory.ru

ISBN 978-5-4493-0826-9

Содержание

Радянська криптологія
Історія спецзв'язку

Вадим Гребенніков

ISBN 978-5-4493-0826-9
Создано в интеллектуальной издательской системе Ridero

1. Народження радянських криптослужб

1917 рік став переломним не тільки в історії Росії, але й усього світу. Країна була розколота на два конфронтуючі табори. Як й інші верстви населення, фахівці-криптологи виявилися «по різні боки барикад». Однак основна їхня частина після революції перейшла на бік супротивників радянської влади.

Тому, незважаючи на те, що у розпорядження радянської влади потрапили майже всі шифродокументи «*цифирных*» підрозділів царської Росії, вони були добре відомі криптологам царської Росії, що працювали на «білих». А фахівці-криптологи, що перейшли на бік радянської влади, під час громадянської війни були розкидані по всій країні.

В результаті використання «царських» і «підпільних» шифрів не могло служити діючим засобом захисту таємної інформації Радянської республіки. Керівники республіки розуміли, що необхідно вкрай «архіважливо й досить терміново» створювати свої власні шифрувально-секретні служби.

Вже у грудні 1917 року в структурі наркомату закордонних справ (далі – НКЗС) Радянської республіки з'явився «Відділ шифрувальний і друкарський». А 29 квітня 1918 року він був реорганізований у самостійний Шифрувальний відділ. Після реорганізації наркомату в серпні 1918 року, коли Канцелярія НКЗС у справах Заходу була перейменована у Відділ Заходу, в нього було включено також і «шифрувальне відділення».

В структурі Робітничо-Селянської Червоної Армії (далі – РСЧА) на початку травня 1918 року обов'язки з шифрування та розшифрування телеграм покладені на Загальне відділення Військово-статистичного відділу Оперативного управління Всеросійського головного штабу (далі – ВГШ) РСЧА.

Разом із цими структурами активно використовувати засоби криптології розпочали й органи Всеросійської надзвичайної комісії з боротьби з контрреволюцією, саботажем і злочинами (далі – ВНК). Так, у прийнятому 11 червня 1918 року «Положенні про надзвичайні комісії на місцях» був 36-ий пункт, у якому говорилося про те, що «для таємних стосунків губернських комісій, надзвичайних комісій з ВНК, виробляється певний шифр, шляхом якого й відбуваються стосунки».

При цьому, структури місцевих органів ВНК на той час ще не передбачали ні окремого шифрувального підрозділу, ні посади шифрувальника. Шифри повинні були зберігатися у керівника місцевого органа ВНК або його заступника. Саме він персонально відповідав за таємність шифрів.

Крім того, у функції ВНК входило проведення контролю за іноземним листуванням. Органи ВНК організували, за прикладом відповідних служб царській Росії, службу перлюстрації шифрованої кореспонденції акредитованих у Москві представників деяких іноземних держав. Відомо, що вже на початку 1920-х років у Москві знаходилися дипломатичні і торгові посольства і місії Німеччини, Англії, Туреччини, Італії, Фінляндії, Польщі, Ірану, Афганістану і прибалтійських держав.

Окрім телеграм, що поступали з телеграфу, частина шифрованого іноземного листування і листування білої гвардії за завданнями ВНК і військових органів перехоплювалася на Серпуховській приймальній радіостанції Революційної військової ради республіки (далі – РВРР) та Шаболовської радіостанції Наркомату пошт і телеграфів. Ці повідомлення разом з перехопленням відкритих повідомлень іноземної преси прямували в так званий «відділ обробки матеріалів» Особливого відділу ВНК.

У відділі обробки матеріалів робилися спроби розшифрувати перехоплені радіограми, отримані при обшуках і арештах членів контрреволюційних організацій шифровані документи. В окремих випадках це вдавалося зробити. Однак більшість шифродокументів, що надходили

у відділ, залишалася не розшифрованою. Стосовно дипломатичного шифрованого листування, то воно зовсім не читалося.

Потребувала своїх шифрувально-дешифрувальних підрозділів також і військова розвідка. Тому 8 листопада 1918 року наказом по ПШ РВРР №46 відповідно до наказу РВРР №197/27 від 5 листопада у складі утвореного Реєстраційного (розвідувального) Управління (скорочено російською *«Региструпр»)* були введені посади «завідувача шифром» і його помічника (В. Панін і П. Озолін відповідно). А 13 листопада того ж року Наказом РВРР №217 було створено шифрувальне відділення звітно-організаційного відділу Організаційного управління ВГШ РСЧА із штатом 14 осіб.

19 червня 1919 року у затвердженому новому штаті *«Региструпра»* ПШ РВРР з'явилася «шифрувальна частина» (начальник – В. Панін, його заступник – П. Озолін). А у вересні 1920 року у затвердженому новому штаті *«Региструпра»* з'явилися шифрувальне відділення (начальник – П. Озолін) і відділення зв'язку (начальник – Вольдемар Янович Закіс).

Будучи зацікавленою у використанні даних шифролистування, ВНК направляла матеріали для дешифрування у військові органи. Ось один з таких документів: «У Польовий штаб Реввійськради Республіки. 14.IV.1920. Згідно з резолюцією начальника відділу обробки матеріалів Особливого відділу ВНК при цьому супроводжуються три копії перехоплення ворожих радіограм від 3 і 4 квітня з проханням розшифрувати в терміновому порядку і повернути у відділ обробки матеріалів ОВ ВНК».

Через 20 днів, 4 травня 1920 року, у Польовий штаб (далі – ПШ) РВРР був надісланий вторинний запит з цього питання. І лише в червні була отримана типова для подібної ситуації того часу відповідь: «Зважаючи на неможливість встановити ключ до цих телеграм останні повертаються в нерозшифрованому вигляді…».

У той же час були створені аналогічні шифрувальні структури в Головному артилерійському управлінні, Управліннях зв'язку, постачання, військових повідомлень й інших. У більш низових ланках управління шифрувальних органів, як такого, не було та вся робота з даного питання велася, як правило, за сумісництвом, без належних норм таємності та конспірації, найчастіше неосвіченими та непідготовленими належним чином людьми.

На лініях зв'язку Радянської республіки, в основному, застосовувалися шифри простої та пропорційної заміни. У період боротьби з адміралом Врангелем радянською стороною застосовувався шифр «Республіка», що являв собою шифр Віженера з чередуванням букв алфавіту усередині квадрата відповідно до ключа-гасла. Не менш широко застосовувалися шифри «Москва» і «Секунда».

Шифр «Москва» також являв собою шифр Віженера, де як гасло використовувався той же відкритий текст, але зрушений на один крок вправо, інакше процес дешифрування був би неможливий. При цьому перша буква гасла була заздалегідь обговореною та мінялася відповідно до розкладу.

Шифр «Секунда» був звичайним шифром заміни на 9, 2, 13 колонок. У 19191920 роках були розроблені та застосовувалися більш стійкі шифри «Кулемет», «Агітатор» та інші, що лише незначно поліпшили несприятливу в цілому ситуацію з забезпеченням таємниці шифролистування в Радянській республіці.

Але й ці швидкі розробки будувалися за старими принципами та не забезпечували захист таємниці. Перехоплені радіоповідомлення РСЧА легко дешифровувались. Так, наприклад, генерал-майор Дентервиль, що командував експедиційними військами Антанти в Персії та Баку в 1918 році, у своїх спогадах писав, що завдяки використанню «червоними» на Каспійському морі старого царського коду, копія якого малася в його штабі, англійським військам удалося одержати важливу інформацію про дії РСЧА. Ця інформація істотно вплинула на хід бойових дій та дозволила англійцям зайняти Баку та інші райони Кавказу.

Відомо, що у період з 1918 по 1920 рік майже всі шифровані радянські військові та дипломатичні повідомлення успішно читалися білогвардійцями, поляками, англійцями, шведами. Так, у серпні – вересні 1919 року шифрувальники Генерального штабу польської армії розкрили шифри РСЧА. У серпні 1920 року вони дешифрували 410 таємних телеграм, підписаних Троцьким, Тухачевським, Гаєм і Якіром. З серпня 1919 і до кінця 1920 року польські шифрувальники розшифрували декілька тисяч радіограм РСЧА, в основному, накази керівництва армії з управління військами.

Крім того, польські шифрувальники нав'язували помилкові накази командирам військових з'єднань РСЧА за допомогою телеграм, зашифрованих військовим шифром РСЧА. їм вдалося перехопити та розшифрувати спеціальну директиву Головнокомандувача Каменєва про те, що 1-а і 2-а Кінні армії повинні бути підпорядковані командувачу Західним фронтом Тухачевському та наступати на Люблінському напрямі. Змінивши її зміст, вони склали фальшиву шифровку від Каменєва зі вказівкою 1-ій Кінній армії йти в наступ на Львів.

В результаті управління військами РСЧА було абсолютно порушене, що привело до їх повного розгрому. Коли б не ця помилкова команда, РСЧА могла б звитяжно завершити свій наступ. Те, що польські розвідслужби змогли порушити управління РСЧА за допомогою помилкових наказів, підтверджується наявністю величезного числа полонених червоноармійців – близько 100 тисяч осіб, що склало, приблизно половину чисельності військ РСЧА, що брали участь у цій битві. Ця битва, названа «Дивом над Вислою», увійшла до списку 18 найбільш видатних переломних битв у світовій історії.

Також перехоплювалося та дешифровувалося листування радянського уряду з делегацією на переговорах у Брест-Литовську. Ретельно відбиралася та аналізувалася інформація про діяльність ВНК. Завдяки радіоперехопленню та дешифруванню керівники «білого руху» контролювали операції РСЧА на Східному та Туркестанському фронтах, стежили за зв'язком командування цих фронтів з Москвою. Навесні 1919 року адмірал Колчак писав російському послу в Греції: «Єдиним джерелом інформації нам служать перехоплені більшовицькі радіо».

Системи шифрування, що застосовувалися військами Будьонного та Куйбишева в Середній Азії, іноді «розколювалися», навіть, «басмацтвом». Слабка професійна підготовка кадрових працівників шифрослужби РСЧА не могла забезпечити належного рівня захисту переданої інформації. Допускалося безліч порушень та послаблень при шифруванні. Так, для економії часу найчастіше шифрувалися тільки окремі ділянки повідомлення тексту, а інша його частина передавалася відкрито.

Вкрай погані були справи в Радянській країні з дешифруванням іноземного та військового листування. У РСЧА не було організованої дешифрувальної служби, тому що створені при штабах шифрогрупи мали головною задачею створення шифрів і захист ними таємного листування. Можна сказати, що дешифрувальна служба практично була відсутня. У той період Радянська держава не мала в розпорядженні сили та засоби для успішного проведення такої роботи.

Разом з тим, наприкінці 1917 року був виявлений архів посольства Англії, в якому були діючі англійські шифри. У результаті радянськими криптоаналітиками був дешифрований ряд телеграм англійського посла в Росії Б'юкенена, а потім і дипломатичного агента Англії Локкарта, що його замінив. Це допомогло ВНК розкрити змову останнього, спрямовану проти більшовиків. У цій змові, метою якого була організація повстання в Москві та фізичне усунення керівництва Радянської республіки, брали участь посли ряду західних країн. Цікаво відзначити, що всі подробиці розкриття змови Локкарта стали відомі білогвардійцям з перехоплених та дешифрованих радянських радіопередач.

Аналогічним чином був виявлений шифр румунського військового аташе. У результаті був розкритий план генерала Корнілова щодо здачі Риги німцям і отримані інші важливі матеріали.

У 1920 році при розгромі армії Врангеля в Криму був захоплений начальник станції радіоперехоплення Ямченко. Він дав згоду співробітничати з новою владою та розповів про практично повне дешифрування «білими» перехоплених повідомлень. З цими даними був ознайомлений Михайло Фрунзе, головнокомандувач Південною групою РСЧА. Ось яку оцінку стану справ у сфері криптографічного захисту інформації в Радянській республіці він дав:

«… З наданого мені колишнім начальником врангельської радіостанції Ямченком доповіді встановлюється, що всі наші шифри внаслідок їхньої нескладності читаються нашими ворогами. Весь наш радіозв'язок є чудовим засобом орієнтування супротивника. Завдяки тісному зв'язку з шифрувальним відділенням морфлота Врангеля, Ямченко мав можливість особисто читати цілий ряд наших шифровок найбільш секретного військово-оперативного та дипломатичного характеру; зокрема, секретне листування Наркомінсправа з його представництвом у Європі та у Ташкенті слово в слово відоме англійцям, що спеціально організували для підслуховування наших радіо цілу мережу станцій особливого призначення. До шифрів, що не піддавалися негайному злому, надсилалися ключі з Лондона, де на чолі шифрувального відділу поставлений англійцями російськопідданий Фетерлейн, що відав колись цією справою в Росії. Загальний висновок такий, що всі наші вороги, зокрема, Англія, були постійно в курсі всієї нашої військово-оперативної та дипломатичної роботи…».

Ось як охарактеризував таку ситуацію нарком закордонних справ Григорій Чичерін у своєму листі Голові Ради Народних Комісарів (далі – РНК) Володимиру Леніну від 21 серпня 1920 року:

«Я завжди скептично відносився до наших шифрів, найбільш таємні речі зовсім не повідомляв і кілька разів застерігав інших від повідомлення таких. Не вірна думка тов. Каменєва, що важко дешифрувати. Від нашого співробітника Сабаніна, сина старого дешифрувальника Міністерства закордонних справ, ми знаємо, що всі іноземні шифри розшифровувалися російськими розшифровувачами. В останній період існування царату не було іноземної депеші, яка б не розшифровувалася, при цьому не внаслідок зрадництва, а внаслідок мистецтва російських розшифровувачів. При цьому іноземні уряди мають більш складні шифри, ніж уживані нами. Якщо ключ ми постійно змінюємо, то сама система відома царським чиновникам і військовим, що знаходяться в стані білогвардійців за кордоном. Розшифрування наших шифровок я вважаю цілком припустимим».

У той же день, 21 серпня, В. Ленін склав термінову відповідь: «Пропоную:

1) змінити систему негайно;

2) змінювати ключ щодня, наприклад, відповідно до дати депеші або відповідно до дня року (1-ий … 365-ий день і т. д. і т.п.);

3) змінювати систему або подробиці її щодня (наприклад, для букви 5 цифр; одна система: перша цифра фіктивна; друга система: остання цифра фіктивна і т.д.).

Якщо змінювати хоча б щотижня (а) ключ і (б) такі подробиці, то не можна розшифрувати».

Слабка стійкість радянських шифрів була обумовлена ще тим, що в урядовій криптологічній школі Британії, створеній при Адміралтействі у 1919 році, головою секції, що працювала проти Росії, служив Ернест Фетерлейн, літня людина на прізвисько Фетті. У Росії перед революцією Фетерлейн займав пост провідного криптолога, мав ранг адмірала та був царем нагороджений перснем з величезним рубіном за виконання делікатних доручень. Після революції Фетті втік до Англії та успішно «розкривав» слабкі радянські шифрувальні системи.

Завдяки Фетерлейну та його англійським колегам британський уряд читав значну частину найважливішого дипломатичного листування росіян під час англо-радянських торгівельних переговорів. Перехоплена інформація мала надзвичайно важливе значення. Так, на самому початку переговорів у червні 1920 року Ленін писав Красіну: «Ця свиня Лойд Джордж піде на обман без тіні сумніву або сорому. Не вірте жодному його слову та у три рази

більше дуріть його». Лойд Джордж філософськи ставився до подібних образ. Однак деякі з його міністрів відносилися до цього інакше. Керзон і Черчилль, використовуючи розшифровану інформацію про фінансову допомогу газеті «Дейлі геральд» і англійським «більшовикам», а також про інші форми радянської підривної діяльності у Великобританії та Індії, вимагали вислати радянську делегацію та припинити торгівельні переговори.

Не бажаючи підривати перспективи досягнення торгівельної угоди, Лойд Джордж, проте, вважав необхідним відреагувати на праведний гнів своїх міністрів, причина якого крилася в розшифрованих документах, що свідчили про підривну діяльність «більшовиків». 10 вересня прем'єр-міністр звинуватив Лева Каменєва, що прибув у Лондон у серпні як керівник радянської торгівельної делегації (у той час Красін був його заступником), у «грубому порушенні даних обіцянок» та у використанні різних методів підривної діяльності. Красіну дозволили залишитися.

Каменєву ж, який наступного дня повинен був повернутися в Росію для одержання нових інструкцій, було оголошено, що йому не буде дозволено в'їхати назад у Великобританію. Лойд Джордж заявив йому, що він має незаперечні докази, які підтверджують висунуті проти нього обвинувачення, однак відмовився повідомити, які саме.

Вочевидь, радянська делегація все-таки зрозуміла, що її телеграми були перехоплені та розшифровані. А вже в серпні Кабінет Міністрів Великобританії дав згоду на публікацію частини перехопленої інформації. 8 розшифрованих телеграм, які доводили, що радянський уряд надавав фінансову допомогу газеті «Дейлі геральд», були передані до редакцій всіх загальнонаціональних газет, за винятком самої «Дейлі геральд». Для того, щоб ввести в оману росіян щодо джерела інформації та спробувати переконати їх у тому, що витік відбувся в Копенгагені в оточенні Максима Литвинова, цей матеріал був переданий у газети з умовою посилання на «нейтральну» країну. Однак газета «Таймс» не прийняла умов гри. До крайнього невдоволення Лойда Джорджа, вона почала свою статтю з наступних слів: «Ці радіограми були перехоплені британським урядом».

10 вересня 1920 року Леонід Красін написав з Лондона листа Леніну:

«Ще в травні при перебуванні в Копенгагені за деякими ознаками я почав підозрювати, що з шифрованим листуванням через Наркомінсправ не все йде благополучно. У Англії ці підозри зміцнилися, і в подальший мій приїзд до Москви я звертав увагу тов. Чичеріна на необхідність корінного чищення у відповідному відділі… Нарешті, сьогодні ми майже офіційно сповіщені, що таємні наші депеші зовсім не є таємницями для Велпра [уряд Великобританії]. Справа не в провалі шифру або ключа, а в тому, що в Наркомінсправ неблагополуччя, так би мовити, абсолютне і змінювати це треба радикально… Здається, виправити справу можна тільки створенням при Наркомінсправ шифрувального відділення незалежно від самого Комісаріату і персонально підібраного з людей або по партії, або особисто відомих протягом десятка – півтора років… Крім того, треба завести особливий ключ з Оргбюро або Політбюро і особливо важливі депеші посилати цими ключами, абсолютно епатуючи К [омісаріа] т у справі їх розшифрування. Не думайте, що все це зайва недовіра, ні, справа дуже серйозна…».

Однак сам Ленін зовсім не розділяв підозри Красіна щодо зрадництва в НКЗС. 25 листопада 1920 року він знову звернувся до Чичеріна: «Питанню про більш суворий контроль за шифрами (і зовнішньому, і внутрішньому) не можна давати заснути. Обов'язково черкніть мені, коли всі заходи будуть прийняті. Необхідне ще одне: з кожним важливим послом (Красін, Літвінов, Шейнман, Йоффе і т.п.) встановити особливо суворий шифр тільки для особистої розшифровки, тобто тут шифруватиме особливо надійний товариш, комуніст (можливо, краще при ЦК), а там повинен шифрувати або розшифровувати особисто посол (або „агент“), не маючи права давати секретарям або шифрувальникам. Це обов'язково (для особливо важливих повідомлень, 1—2 рази на місяць по 2—3 рядки, не більше)».

Відповідь була дана наступного дня: «Узагалі питанням про кращу постановку шифрувальної справи в Республіці займається комісія тов. Троцького… Єдиний особливо суворий шифр є книжковий. Користуватися книжковими шифрами можна лише в окремих випадках унаслідок крайньої громіздкості цієї системи. Потрібно занадто багато часу. Для окремих найбільш таємних випадків це можна робити. На початку всі наші кореспонденти мали книги, але внаслідок занадто великої громіздкості цієї системи поступово відмовилися. Можна буде відновити цю систему для окремих випадків, користуючись помилками для повідомлення кореспондентів…».

Після цього радянська торгівельна делегація в Лондоні одержала інструкцію пересилати свою кореспонденцію, по можливості, кур'єрською поштою до розробки нової системи шифру. Фетерлейн і його англійські колеги протягом декількох місяців не могли розгадати нові радянські шифри, введені в дію на початку 1921 року. Але вже до кінця квітня вони змогли розшифрувати значну частину радянського дипломатичного листування.

Радянські агентурні шифри були тоді слабші ніж дипломатичні. Так, завербований у паризькому центрі білогвардійського руху агент скаржився на слабкість і незручність шифрів, що використовувались. Найбільш пунктуального офіцера російської армії дратувало те, що шифровки наносилися тайнописом між рядків звичайних послань, а Москва нерідко забувала спеціальним чином по значити лист, що містив тайнопис, і він знищувався без прочитання. Більше того, виявлений поганим складом тайнописний текст зникав часом так швидко, що не вдавалося встигнути його скопіювати.

1 вересня 1920 року Чичерін написав листа наркому фінансів Крестинському про направлення в НКЗС співробітників для роботи в шифрувальному відділенні: «Наші шифрувальники були і раніше переобтяжені роботою, а зараз створилася повна невідповідність між їх складом і роботою. Збільшення складу наших шифрувальників є тепер завданням першорядної ваги».

А 16 вересня 1920 року він написав листа Леніну про «обережність із питання про персонал, пов'язаний з шифровками», і пропонував йому, щоб всі співробітники шифрувального відділення або шифрувальники «були ухвалені Оргбюро і Особливим відділом ВНК». На його думку, було особливо необхідно ретельно підбирати «самокатчиків», які розвозили б шифровки. У інших листах Леніну Чичерін порушив такі питання, як правила розсилки шифротелеграм, їх зберігання, охорони НКЗС, особливо охорони шифрувального відділу, для чого нарком пропонував призначити курсантів, «як це практикується у Кремлі».

Того ж місяця Політбюро російської комуністичної партії (далі – РКП) розглянуло «пропозицію т. Леніна вжити заходів щодо ускладнення шифрів і до більш суворої охорони шифрованих повідомлень». Політбюро ухвалило доручення наркому з військових і морських справ Троцькому, *«организовать комиссию из представителей Наркомвоєна, Наркоминдела, ЦК РКП и Нар-компошителя»*. Ленін, вивчивши досконало питання, знаючи думку НКЗС й інших зацікавлених відомств, доручив знайти шляхи наведення порядку в шифрувальній справі керівництву ВНК, хоча шифрувальні служби були й у інших наркоматах.

Одразу ж почала працювати Державна комісія з питання «постановки шифрувальної справи в Республіці». У зв'язку з цим Чичерін 25 вересня 1920 року доповідав у РНК, що «з понеділка у нас розпочне працювати т. Голуб, завдання якого полягатиме в перетворенні шифровок на офіційні папери для розсилки їх у такому абсолютно зміненому вигляді звичайним одержувачам».

А вже наприкінці 1920 року в НКЗС був розроблений «Циркуляр про шифри». 1 березня 1921 року завідувачем шифрувальною частиною був призначений І.М.Міхель, колишній завідувач канцелярією НКЗС.

2. Спеціальний відділ ВНК

В десятих числах січня 1921 року Колегія ВНК приймає рішення про скликання наради представників зацікавлених відомств для підготовки відповідних пропозицій щодо утворення єдиної криптологічної служби. В обговоренні питання брали участь представники ЦК РКП, ВНК і наркоматів. В результаті 28 січня 1921 року при ВНК був утворений Спеціальний відділ для координації та контролю відомчих шифрувальних служб і централізованої організації секрет ного діловодства у державних установах. Відділ очолив колишній голова Петроградської НК у 1918 році та повноважний представник ВНК у Туркестані у 191920 роках Гліб Іванович Бокій, який з 12 липня 1921 року увійшов за посадою до Колегії ВНК.

Колегія ВНК до березня підготовила пропозиції про створення міжвідомчої шифрувальної комісії при РНК, що складалася з представників Наркомата військових справ, ВНК, НКЗС і Наркомата зовнішньої торгівлі під головуванням представника ВНК – начальника Спеціального відділу. Проте розроблений ВНК проект діяльності цієї комісії прийнятий не був, оскільки стало очевидно, що в умовах, що створилися, за наявності у всіх наркоматів безлічі важких невідкладних власних завдань, всю роботу зі створення і організації діяльності спеціальної служби повинно узяти на себе одне відомство, а саме ВНК.

Було прийнято ухвалу, запропоновану Леніним: «Доручити начальнику шифрувального відділу ВНК прийняти заходи до здійснення нагляду, контролю і керівництва шифрувальною справою в Республіці і представити в Малу раду відповідний проект Ухвали, погодивши його з найбільш зацікавленими відомствами». 12 квітня на засіданні Малого РНК з проектом утворення єдиного у країні шифрувально-дешифрувального відділу виступив начальник Спеціального відділу при ВНК Бокій, людина, якій належало стати головним організатором криптологічної служби країни і її першим керівником.

Ось текст цього проекту:

«Маючи на увазі: 1) відсутність у Республіці центру, що об'єднує та спрямовує діяльність шифрувальних органів різних відомств, і пов'язані з цим безсистемність і випадковість у постановці шифрувальної справи; 2) можливість, завдяки цьому, при існуючому положенні широкого інформування ворогів Робітничо-селянської держави про таємниці Республіки, Рада Народних Комісарів ухвалила:

Утворити при Всеросійській Надзвичайній Комісії «Спеціальний відділ», штати в якому затверджуються Головою ВНК. Начальник Спеціального відділу призначається Раднаркомом.

У коло ведення Спеціального відділу при ВНК включити:

I. Постановку шифрувальної справи в РРФСР:

А. Наукова розробка питань шифрувальної справи:

а) аналіз всіх існуючих та існуючих російських і іноземних шифрів;

б) створення нових систем шифрів;

в) складання описів шифрів і інструкцій у шифрувальній справі та користуванні шифрами;

г) збирання архівів і літератури у шифрувальній справі для сконцентрування такого при Спецвідділі;

д) складання і видання керівництва з питань шифрування. *Б. Обстеження і вироблення систем шифрів:*

1. Обстеження всіх шифрів, що діють у даний час, і порядку користування ними шифрорганами;

2. Остаточна обробка інструкцій у шифрувальній справі і користуванні шифрами та розробка правил роботи шифрорганів;

3. Розподіл знов вироблених систем шифрів між всіма відомствами. В. Організація навчальної частини:

1. Розробка програми школи шифрувальників.

2. Створення школи шифрувальників.

3. Укомплектовування школи викладачами і учнями.

Г. Облік особового складу шифрувальних органів. Спостереження за закономірною постановкою шифрувальної справи. Інструктаж та інспекція шифрувальних органів:

1. Облік і перевірка всіх співробітників всіх шифрорганів.

2. Розподіл співробітників усіх шифрорганів між останніми залежно від індивідуальних якостей кожного працівника та фактичної потреби в працівниках у тому або іншому шифрогані, а також залежно від державної важливості кожної установи.

3. Чищення неблагонадійного і нездібного елементу зі всіх шифрорганів.

4. Спостереження за закономірною постановкою шифрувальної справи у всіх шифрорганах.

5. Інструктаж та інспекція всіх шифрорганів і проведення в життя Інструкції і правил у шифрувальній справі.

II. Постановка розшифрувальної справи у РРФСР:

1. Дослідження способів повсюдного вловлювання всіх радіо, телеграм і листів ворожих, іноземних і контрреволюційних.

2. Відкриття ключів ворожих, іноземних і контрреволюційних шифрів.

3. Розшифровка всіх радіо, телеграм і листів ворожих, іноземних і контрреволюційних.

Всі розпорядження і циркуляри Спеціального відділу при ВНК з усіх питань шифрувальної та розшифрувальної справи є обов'язковими до виконання всіма відомствами РРФСР».

Тим часом 4 квітня 1921 року наказом РВРР №785/141 *«Региструпр»* ПШ РСРР був реорганізований у Розвідувальне Управління (далі – РУ) Штабу РСЧА. У його складі було створене шифрувальне відділення 2-го (агентурного) відділу, начальником якого став В.Я.Закіс.

А вже 5 травня 1921 року постановою Малого РНК №672 була утворена єдина радянська криптослужба у вигляді Спеціального відділу при ВНК. Приведемо текст цієї постанови:

«РНК, розглянувши питання про шифрувальні відділи, ухвалив наступне:

1) утворити при ВНК «спеціальний відділ»;

2) Спецвідділ ВНК поєднує всі шифрувальні органи, контролює й направляє всю діяльність таких органів;

3) всі розпорядження й циркуляри Спецвідділу ВНК із всіх питань шифрувальної та розшифрувальної справи є обов'язковими до виконання всіма відомствами Росії».

З того часу 5 травня вважається святом шифрувальників усіх міністерств і відомств. Начальником нової структури й одночасно членом колегії ВНК був призначений Гліб Іванович Бокій, який до цього керував Петроградською НК і завжди цікавився шифруванням, а свої записи про підпільні справи шифрував особистим математичним шифром.

З його ініціативи 25 серпня 1921 року у ВНК був виданий наказ, що пропонував усім підрозділам у центрі та на місцях «направляти в Спецвідділ всякого роду шифри, ключі до них і шифровки, виявлені при обшуках та арештах, а також добуті через агентуру або випадково».

Розміщався відділ не тільки на Малій Лубянці, але й у будинку №21 на вулиці *«Кузнецкий мост»,* у приміщеннях НКЗС, де займав два верхні поверхи. Офіційними його завданнями були масштабна радіо- і радіотехнічна розвідка, дешифрування телеграм, розробка шифрів, радіоперехоплення, пеленгація й виявлення ворожих шпигунських передавачів на радянській території.

Специфіка роботи Спецвідділу докорінно відрізнялася від усього того, що робилося у ВНК, а тому вимагала залучення людей, що володіли унікальними навичками. Це насамперед відносилося до криптологів, завданням яких було розгадування шифрів і ребусів.

Взагалі, серед особового складу дешифрувального відділу було багато колишніх російських аристократів, зокрема графів і баронів. Ця суперечність із державним устроєм того часу пояснювалася серйозним браком лінгвістів, які були потрібні для ведення дешифрувальних робіт. А сама професія дешифрувальника була настільки рідкісною, що навіть тоді, коли представники цієї професії потрапляли у в'язницю, їх все одно залучали до роботи за фахом.

Ось що розповів письменник Лев Разгон, який був зятем Бокія, а в 1930-і роки – співробітником Спецвідділу: «Бокій підбирав людей дуже різних і дивних. Як він підбирав криптографів? Адже це здатність, що дана від Бога. Він спеціально шукав таких людей. Пам'ятаю старого співробітника Охоронки статського радника (у чині полковника), що ще в Петербурзі, сидячи на Шпалерній, розшифрував таємне листування Леніна. У відділі працював і винахідник-хімік Євгеній Гоппіус. У ті часи найважчим у шифрувальній справі вважалося знищення шифрувальних книг. Це були товсті фоліанти, і потрібно було зробити так, щоб у випадку провалу або інших непередбачених обставин подібні документи не дісталися ворогу. Наприклад, морські шифрувальні книги мали свинцеве плетіння, і в момент небезпеки військовий радист повинен був кинути їх за борт. Але що було робити тим, хто знаходився вдалині від океану та не міг оперативно знищити небезпечний документ? Гоппіус же придумав спеціальний папір, і треба було тільки піднести до нього у відповідальний момент палаючу цигарку, як товста шифрувальна книга перетворювалася через секунду в купку попелу».

До служби у Спецвідділі у першу чергу залучались колишні «царські» криптологи. Так, у 1919 році перекладачем-дешифрувальником Особливого відділу ВНК був призначений відомий нам Володимир Іванович Крівош, а його син Роман – секретарем бюро з видачі перепусток у прикордонну зону Особливого відділу Московської НК. У цей час Володимир Іванович додав до свого прізвища слово «Неманіч» (скорочено – нема нічого), мабуть, підкреслюючи цим своє матеріальне становище порівняно до царського часу. Тепер він мав прізвище – Крівош-Неманіч.

У 1920 році він разом із сином Романом був арештований ВНК за підозрою у організації незаконного перетинання кордону. Однак у тому же році Роман був звільнений за амністією, а Володимир Іванович – у 1922 році та прийнятий на службу у Спецвідділ у якості експерта. Цікаво, що його син Роман з 1 травня 1921 року вже працював перекладачем-дешифрувальником Спецвідділу.

У 1923 році Крівош-Неманіч був арештований за підозрою у шпигунській діяльності та висланий на 10 років у Соловецький концтабір. У 1928 році він вийшов на свободу та знову став працювати експертом у Спецвідділі. У 1935 році Крівош-Неманіч був звільнений на пенсію, а у 1937 році був арештований його син Роман, співробітник Спецвідділу ГУДБ НКВС.

Завдяки своїм високим професійним здібностям Роман до концтаборів висланий не був і знаходився у Бутирській в'язниці, де успішно працював криптологом. З початком Вітчизняної війни у 1941 році Роман був звільнений та разом з батьком мешкав у евакуації в Уфі. Роман Крівош продовжував свою службу як фахівець-криптограф Спецвідділу НКВС і у 1942 році був нагороджений медаллю «За трудову відмінність». Його батько Володимир Іванович Крівош-Неманіч помер 4 серпня 1942 року в Уфі.

Штатним співробітником Спецвідділу став і талановитий криптолог «охоронки» Іван Зибін. Ще довгі роки він успішно працював у криптослужбі, допомагаючи створювати вже радянську школу криптологів. Перед молодими співробітниками він не боявся розповісти, що у свій час дешифрував деякі листи Леніна! Утім, справа ця була не дуже складною… Подальша його доля на даний час залишається невідомою.

Робота Спецвідділу розпочалася з детального вивчення спадку, отриманого з архівів спеціальної служби дореволюційній Росії. Це були шифри, їх детальний опис, документи з дешифрування, матеріали шифроперехвату. Серед цих документів, зокрема були матеріали з дешифрування шифрів Туреччини, Персії, Японії, інших держав, а також копії і оригінали шифрів США, Німеччини, Японії, Китаю, Болгарії, навчальні посібники тощо.

Співробітники відділу ретельно вивчали ці матеріали, усвідомлюючи важливість своєї роботи. Велику роль в цей і подальший періоди зіграли знання і досвід Зибіна, Крівошa-Неманіча та інших «царських» криптологів. При їх активній участі при Спецвідділі були організовані 6-місячні курси, на яких вивчалися основи криптографії, вирішувалися завдання з дешифрування. На курси набирали людей здібних і грамотних. Перший випуск курсів складався з 14 осіб, п'ятеро з яких пришли на роботу в дешифувальне відділення відділу, останні – в інші відділення.

Необхідною умовою успішної роботи Спецвідділу була наявність матеріалів шифроперехвату. У способах їх отримання зберігалися традиції дореволюційних служб. Окрім зняття копій з шифровок іноземних держав, що проходили через Центральний телеграф або доставлялися дипломатичною поштою, чим займався відділ Політконтроля, було посилено перехоплення шифротелеграм, що передавалися по радіоканалах. З цією метою були задіяні військові радіостанції, надані в розпорядження Спецвідділу радіомовні станції, зокрема радіостанція Комінтерну. Однак недосконаліть радіоприймальної апаратури, а також сильна зношеність не могли забезпечити високої достовірності текстів перехоплених шифротелеграм.

Таким чином до труднощів перших років роботи Спецвідділу, пов'язаних із невисокою загальною підготовленістю та нечисленністю особового складу, додавалися труднощі, пов'язані з недоліком і низькою якістю матеріалів для дешифрування. Перед керівництвом Спецвідділу постали завдання організації та налагодження роботи всіх ланок спеціальної служби в країні, включаючи здобуття шифроматеріалів і технічне оснащення радіостанцій. У зв'язку з цим Спецвідділом проводилася робота з розробки та виготовлення спеціальної техніки. У тісному контакті працював Спецвідділ з Закордонним відділом ВНК, контактуючи та маючи зв'язок з агентурою, орієнтованою на здобуття шифрів і кодів.

Зберігся звіт про роботу Спецвідділу за 1921 рік. У ньому, зокрема, було вказано, що з самого початку успішно проводилася розробка та виготовлення нових кодів і шифрів. Тільки за цей рік було введено в дію на різних лініях зв'язку 96 нових кодів. Ця робота співробітників Спецвідділу активно підтримувалася урядом. Характерною для того часу була телеграма секретаря ЦВК СРСР Єнукідзе Бокію, хоча і відносилася вона вже до 2 вересня 1924 року та була пов'язана з закінченням роботи над телеграфним кодом:

«Поздоровляю тов. Г.І.Бокія з закінченням складання «Російського коду» – цієї величезної і складної праці.

«Буття визначає свідомість». Буття і необхідність сучасних стосунків, швидкий зв'язок і економія в часі штовхнули людей до створення цієї нової мови «коду», мови, не схожої ні на одну людську мову.

Як маленький шматочок радію при розкладанні випускає колосальну кількість енергії, так і слова «коду» – короткі, незрозумілі і невимовні для нашої мови, при розшифруванні розгортають перед нами ряд фраз і думок, що посилаються або отримуються нами здалеку.

Як стенографія стала необхідною для точного запису і розмноження людської мови, так і мова «код» стає і повинна стати необхідною в стосунках між людьми, що знаходяться на різних точках земної кулі.

Я упевнений, що «код» отримає широке застосування в усіх наших установах Союзу РСР.

Раз темп роботи Жовтневої революції нас привів до того, що ми вимушені були красиву та гнучку російську мову вимовляти зі скороченням складів, то по дротах і повітряних хвилях

ми сміливо спілкуватимемося концентрованою мовою «код», тим паче, що вона доходитиме до адресатів у красивому, розгорненому і зрозумілому вигляді.

Я зі свого боку закликаю всі установи ввести у себе при спілкуванні по телеграфу і радіо мову «код». Єнукідзе».

На початку 1920-х років Спецвідділ включав 6, а пізніше – 7 відділень. Проте власне криптографічні завдання вирішували тільки три з них: 2-е, 3-є і 4-е. Так, співробітники 2 відділення займалися теоретичною розробкою питань криптографії, виробленням шифрів і кодів для ВНК і всіх інших установ країни (включаючи МЗС, Військове відомство тощо). Відділення в перші роки роботи складалося з 7 осіб, а його начальником був Федір Григорович Тіхоміров.

Перед 3 відділенням стояло завдання «ведення шифроробoти та керівництво цією роботою у ВНК». Складалося воно спочатку всього з 3-х осіб, керував відділенням старий більшовик, колишній латиський стрілець Федір Іванович Ейхманс, який одночасно був заступником начальника Спецвідділу. Ейхманс організовував шифрозв'язок із закордонними представництвами СРСР, спрямовував і координував їх роботу.

Співробітники 4 відділення, а їх було 8 осіб, серед яких був і Крівош-Неманіч, займалися «відкриттям іноземних і антирадянських шифрів і кодів та дешифровкою документів». Начальниками цього відділення були: з травня по грудень 1921 року – Ященко, з січня по серпень 1922 року – Горячов, з серпня 1922 по вересень 1923 року – Ельтман.

Перші успіхи радянських криптослужб незабарилися. Уже в 1921—22 роках удалося розкрити перші дипломатичні й військові турецькі шифри, до 1925 року проводилася активна й небезуспішна робота з шифрами 15 європейських держав, у 1927 році розпочалося читання японських повідомлень, а в 1930 році були розкриті деякі шифри США.

У травні 1921 року при Штабі РСЧА був також утворений свій спецвідділ -Центральний шифрувальний відділ (далі – ЦШВ) і було затверджене Положення про нього та його штат, а також штати шифрорганів штабів фронтів, округів, армій, дивізій, бригад, Центрального управління ВОСО і дислокаційне відділення (далі – ДВ) Управління зв'язку штабу РСЧА, Управління ВОСО і ДВ зв'язку штабів фронтів і армій. ЦШВ складався з 4-х відділень загальною чисельністю 27 осіб.

В той час столицею радянської України був Харків, тому в 1921 році в складі українських органів держбезпеки був створений Загальний відділ під керівництвом Ігнатова, одним із завдань якого було забезпечення таємного телеграфного зв'язку. Пізніше при ДПУ Української Радянської Соціалістичної Республіки (далі – УРСР) було організовано Шифрувальне бюро.

Співробітниками ЦШВ були розроблені перші радянські шифри *«74-й Ключ Наркомвоена», «Гелиос», «75-й Ключ Наркомвоена», «Советский»* та інші. У 1921 році ними було виготовлено й розіслано у війська та на флот 54 нові шифри і 2 радіокоди.

Коди та шифри того часу – «Око», «Кулемет», «Стрілок», «Пролетар», «Іскра», «Спартаківець» – згодом були витіснені більш серйозними – «УП Третій», «АРО Перший» та іншими. Це підвищило стійкість шифрованих повідомлень і збільшило безпеку застосування наявних каналів зв'язку.

З перших місяців свого існування Спецвідділ розпочав успішно проводити дешифрування іноземного листування. Колегія ВНК робила все для того, щоб організувати справу найкращим чином і забезпечити повну таємність. Був встановлений порядок, згідно з яким про всі розкриті шифри та здобуті відомості Спецвідділ доповідав ЦК партії, Раднаркому, голові ВНК і керівникам інших зацікавлених відомств.

Колегія ВНК надавала велике значення оперативному використанню таємного листування, що дешифрувалося. Всі термінові і особливо важливі дешифровані повідомлення доповідалися негайно. Вже у той час дешифровані матеріали активно використовувала радянська розвідка, НКЗС, деякі інші організації.

Перший позитивний результат був досягнутий у «розкритті» німецького дипломатичного коду, яким користувався повноважний представник німецького уряду в Москві. Це був цифровий 5-значний код з перешифруванням гамою багатократного використання. Починаючи з червня 1921 року, розшифровувалося все листування на лінії зв'язку Москва-Берлін.

З 1922 року Німеччина ввела на дипломатичних лініях зв'язку буквений код з перешифруванням гамою багаторазового використання. Коди та велика частина перешифрувальних засобів розкривалися аналітичним шляхом у Спецвідділі. Розкриття таких шифрів дозволило контролювати листування багатьох ліній дипломатичного зв'язку Німеччини та її консульств у Ленінграді, Києві, Одесі, Харкові, Тбілісі, Новосибірську, Владивостоку аж до 1933 року, коли кількість читаного листування різко скоротилася через те, що німці почали застосовувати гаму одноразового використання.

У серпні 1921 року було здійснено дешифрування перших турецьких дипломатичних телеграм. Вже на початку 1920-х років криптологи Спецвідділу добилися можливості читати листування внутрішніх ліній зв'язку Туреччини та окремих ліній зв'язку військових аташе. Турки застосовували головним чином 4-значні коди з перешифруванням короткою гамою, змінною через дві доби, а також коди без перешифрування. Дешифроване листування містило відомості, які представляли великий інтерес для радянської сторони, та активно використовувалося. Багато дешифрованих телеграм надсилалося, наприклад, в Закавказьку НК, і це давало можливість вжити заходи з припинення шпигунських дій іноземних, а у даному випадку турецької, розвідок. У 1921 році Спецвідділ розпочав розробляти англійське шифролистування.

Велику допомогу Спецвідділу надавав Іноземний відділ ВНК, розвідники якого у період 1920-30-х років добули більше 10 англійських кодів. По цих шифрах читалася частина дипломатичного листування, проте не вся, оскільки виникали складнощі з розкриттям перешифрування.

Серед «розкритого» листування було багато матеріалів, що представляли великий інтерес для радянського уряду, органів радянської розвідки та контррозвідки. Серед таких документів були, наприклад, телеграми про радянсько-англійські відносини, про продаж англійцями зброї країнам, що мали кордон з СРСР, про діяльність англійської розвідки у Середній Азії тощо.

Хоча робота з розкриття польських шифрів почала проводитися незабаром після організації Спецвідділу, перші практичні результати були отримані лише у 1924 році, коли були розкриті 2 коди 2-го розвідувального відділу генерального штабу польської армії для зв'язку з військовими аташе в Москві, Парижі, Лондоні, Ревелі, Вашингтоні і Токіо.

Для органів державної безпеки особливу цінність мали дешифровані телеграми, що освітлювали шпигунську діяльність кадрових розвідників, що знаходилися під офіційним прикриттям іноземних дипломатичних, військових і консульських представництв у СРСР. Так, почате у 1924 році читання дешифрованого листування польських військових аташе дозволило отримувати таємні повідомлення польської розвідки, яка намагалася широко проводити шпигунську роботу на території СРСР. Радянська розвідка була дуже зацікавлена в отриманні подібної інформації.

Природно, що в початковий період своєї роботи Спецвідділу довелося зустрітися з великими труднощами. Досвідчених криптологів було мало, і кожному з них доводилося очолювати роботу по декількох напрямах. Молоді співробітники ще не володіли необхідними криптологічними та мовними знаннями. Перехоплення шифролистування по багатьох лініях зв'язку велося нерегулярно, можливості виділених технічних засобів були дуже обмежені. Всі роботи, пов'язані з аналізом шифроматериалів, проводилися тільки вручну. Були й інші труднощі. Проте у міру зміцнення Спецвідділу, зростання майстерності його співробітників обсяг криптологічних досліджень з розкриття шифрів почав неухильно зростати. До 1925 року проводи-

лася розробка шифрів вже 15 держав. У 1927 році почалося читання японського листування, а у 1930 році – листування деяких ліній зв'язку США.

Окрім розробки шифрів іноземних держав одним з актуальних завдань дешифрувального відділення Спецвідділу у цей період була розробка так званого внутрішнього шифрованого листування, тобто нелегального листування білогвардійських та інших контрреволюційних організацій, ворожих радянському ладу політичних угрупувань. Архівні документи свідчать, що фахівці 4-го відділення Спецвідділу змогли розкрити сотні різних шифрів, ключів і умовностей. Ними були прочитані тисячі всіляких листів, донесень і інших конспіративних документів, зокрема виконаних тайнописом.

На початку 1920-х років Спецвідділом досліджено багато шифроматеріалів царського Департаменту поліції і жандармерії. Було прочитано 90 документів, за якими складено 10 основних ключів. За дешифрованими матеріалами встановлено багато таємних агентів поліції і жандармерії, що працювали тепер на фабриках і заводах різних міст.

Однією з контрреволюційних організацій, шифролистування якої було вперше дешифроване у 1921 році, був «Народний союз захисту Батьківщини та свободи» Бориса Савінкова. Аналізом ряду шифрованих документів встановлено, що члени цієї організації використовували шифри пропорційної заміни. Незабаром вони були розкриті.

Шифри організації Савінкова будувалися в квадраті 10х10 або були шифрами за словом на довжину алфавіту, рядки ключа чергувалися. Фактично виходили ключі до шифру або в прямокутнику 10х30, або виявлялася 10-значна пере-шифрувальна гама. Було розкрито 26 ключів до шифру та дешифровано більше 30 документів, що містили паролі та конспіративні явки.

У 1922—1924 роках головним чином «розкривалися» матеріали меншовицьких організацій. За ці роки було дешифровано 38 документів і розкрито 17 ключів до шифру. За цими матеріалами було встановлено 65 адрес із паролями та явками.

Перехоплювалося та доставлялося у Спецвідділ листування кримінального розшуку Китайської військової залізниці. Було дешифровано 355 телеграм, розкрито 33 ключі до шифру та один код на 900 величин.

6 лютого 1922 року на базі ВНК було утворене Державне політичне управління (далі – ДПУ) при НКВС. 1 грудня 1922 року був уведений новий штат центрального апарата ДПУ кількістю 2213 осіб, у складі якого залишився Спеціальний відділ з керівництва шифрувальною справою в країні, контролю за діяльністю шифрувальних органів і веденню радіоконтррозвідки (начальник Спецвідділу – Бокій, помічник начальника – Олександр Георгійович Гусєв, начальники відділень – Григорій Карлович Крамфус, Микола Якович Кліменков, Володимир Дмитрович Цибізов).

З того часу органи ДПУ почали приймати суворі заходи з дотримання вимог організації шифрувального зв'язку та забезпечення його безпеки. Спецвідділ ДПУ проводив розслідування фактів порушень порядку зберігання й використання шифрів і надавав рекомендації щодо покарання винних чиновників.

Так, у червні 1922 року Спецвідділ ДПУ розіслав по всіх губерніях повідомлення про недбале зберігання шифродокументів співробітником Володимирського губернського комітету компартії Щолоковим. Спецвідділ рекомендував покарати порушника 15-добовим арештом, причому виконання дисциплінарного стягнення покласти на Володимирський губернський відділ ДПУ.

Організаційний відділ ЦК РКП (б), розглянувши на засіданні 12 червня 1922 року це питання, висловив повну згоду із пропозицією Спецвідділу. Секретар ЦК Йосиф Сталін у супровідному листі, прикладеному до пакета документів про «володимирський інцидент», підтвердив, що й надалі «за всяке порушення інструкції з ведення шифролистування та збері-

гання шифродокументів, як і за порушення елементарних правил конспірації – винні будуть притягнуті до найсуворішої відповідальності».

15 березня 1923 року всім місцевим прокурорам була розіслана шифротелеграма відділу прокуратури Наркомату юстиції, де говорилося про суворе дотримання інструкцій шифрорганами. «Ніяких розмов про шифр із будь-ким без винятку не припустимо. Винні в порушенні цього будуть притягатися до відповідальності». Крім цього, співробітникам, що мали відношення до шифрорганів, заборонялося відвідувати іноземні місії, представництва та торгівельні консульства, а так само мати знайомства зі співробітниками цих органів.

26 травня того ж року був розісланий циркуляр Спецвідділу ДПУ з пропозицією максимально впорядкувати та законспірувати шифрувальну роботу, зокрема: керівникам взяти у осіб, що мають справу із шифродокументами, підписку про відсутність контактів з іноземними місіями та представництвами. У випадку наявності родичів або знайомих в іноземних місіях, співробітники шифрорганів повинні були сповістити про це шифрувальні відділення за місцем роботи.

Крім того, на початку 1923 року в країні були введені нові дипломатичні шифри, які вважались радянськими криптологами стійкими. Однак англійському криптоаналітику «Фетті» знадобилося всього лише кілька днів, щоб прочитати їхній скандальний зміст. Результатом цього став знаменитий «ультиматум Керзона» з вимогою припинити ворожі дії Москви проти Британії.

В опублікованому в травні 1923 року ультиматумі, у якому більшовики звинувачувалися в підривній діяльності, не тільки буквально цитувалися перехоплені радянські радіограми, але й відпускалися досить недипломатичні жарти на адресу росіян із приводу успішного розшифрування перехопленої англійцями їхньої кореспонденції: «У російському Комісаріаті іноземних справ напевно пригадають наступне повідомлення, датоване 21 лютого 1923 року, що було ними отримано від Ф. Раскольнікова… У Комісаріаті іноземних справ також повинні пригадати і радіограму, отриману ними з Кабула і датовану 8 листопада 1922 року… Очевидно, їм знайомо і повідомлення від 16 березня 1923 року, надіслане Ф. Раскольнікову помічником комісара іноземних справ Л. Караханом…».

Влітку 1923 року Москвою були введені нові шифри та коди, над якими Фетерлейну та його колегам знову довелося «поламати голову». Але до кінця 1924 року вони все ж таки знову змогли розшифрувати значну частину радянського дипломатичного листування.

3. Становлення криптослужб СРСР

6 липня 1923 року на території колишньої Російської імперії була утворена нова держава – Союз Радянських Соціалістичних Республік (далі – СРСР) та затверджена її Конституція. 2 листопада того ж року при РНК СРСР було утворене Об'єднане державне політичне управління (далі – ОДПУ), а 15 листопада затверджено «Положення про ОДПУ». На підставі цього Положення ДПУ республік було виведене із підпорядкування республіканських НКВС і було перепідпорядковано безпосередньо ОДПУ при РНК СРСР.

12 листопада 1923 року згідно з новим «Положенням про НКЗС СРСР» його шифрувальна частина була названа «шифрувальною та таємною частиною». Вона вийшла зі складу Управління справами і стала структурною частиною Секретаріату Колегії НКЗС. Однак у цей же період відбувалося скорочення штатів державних установ.

В одному з листів у відповідні органи 31 липня 1923 року нарком Г. Чичерін писав: «*На шифрчасти чрезвычайно тяжело отражаются как колоссальные сокращения, произведенные у нас, так и ужасающе низкие ставки… Мы должны признать безграничную преданность тех партийных товарищей, которые в такой тяжелой обстановке тем не менее до изнурения работают, перенося непосильную тяжесть, лежащую на безмерно сокращенной шифрчасти».*

У цьому ж листі він повідомляв, що новопризначеному члену Колегії НКЗС СРСР В. Л. Коппу доручено «працювати над всіма питаннями з організації в НКЗС шифрувальної справи». Згідно з даними про виконану в 1924 році роботу 2-го відділення таємно-шифрувальної частини НКЗС СРСР значиться, що зашифровано було 309408, а розшифровано 479299 документів.

Що стосується України, то 10 вересня 1924 року Постановою РНК УРСР на базі Шифрувального бюро ДПУ УРСР був утворений Спецвідділ. На нього покладені обов'язки з керування шифрувальною роботою у всіх наркоматах і центральних установах УРСР (крім загальносоюзних), розробки та обліку шифрів, підбору та обліку особового складу шифрувальних підрозділів, загального нагляду за додержанням конспірації у шифрувальній роботі. Постановою РНК УРСР від 24 листопада 1924 року був затверджений його штатний розклад чисельністю у 5 осіб.

28 березня 1924 року на підставі наказу Революційної Військової Ради (далі – РВР) СРСР №446/96 про реорганізацію Центрального апарату наркомату з військових і морських справ (далі – НКВМС) СРСР Центральний шифрувальний відділ Штабу РСЧА був реорганізований у Шифрувальний відділ при РВР СРСР.

У 1925 році начальник Спецвідділу ОДПУ Бокій завдяки своїм успіхам у сфері «таємної війни» зумів зайняти посаду заступника Голови ОДПУ. Він організував зразкову роботу з питань криптології та радіорозвідки. У 1926 році була введена в дію «Інструкція з ведення секретного та шифрувального діловодства».

7 січня 1925 року комісія при таємно-шифрувальній частині НКЗС заслухала доповідь про роботу секретної частини та ухвалила об'єднати секретну й шифрувальну частини та назвати знов створену частину таємно-шифрувальною частиною НКЗС. Через два місяці, 7 березня 1925 року, було ухвалено рішення про ліквідацію секретної частини, а замість неї створити у складі шифрувальної частини 3-е відділення (секретне), а 9 березня 1925 року Колегія НКЗС затвердила це рішення.

У цьому ж році Нарком закордонних справ СРСР Г. Чичерін знов порушує питання про поповнення персоналу шифрувальників. 21 квітня і 8 травня 1925 року він звертається з цього питання в секретаріат ЦК РКП (б): «Недостатність персоналу нашої шифрочастини стає вже державною небезпекою».

У кінці 1925 року секретаріат колегії НКЗС почав функціонувати на правах управління, секретно-шифрувальна частина була перейменована в секретно-шифрувальний відділ, а три відділення, що входили в його склад, перейменовані в перший, другий і третій підвідділи відповідно.

У вересні 1926 року найменування управлінь Штабу РСЧА стали номерними. Військове Розвідувальне Управління перетворилося на IV Управління Штабу РСЧА. Шифрувальне відділення було виведене з складу 2-го (агентурного) відділу та реорганізоване у 1-у (шифрувальну) частину IV Управління, начальником якої став Закіс, а його помічником – Едуард Янович Озолін. Шифрувальний відділ при РВР СРСР був реорганізований у 2-й відділ Управління справами НКВМС і РВР СРСР.

9 грудня 1927 року наказом ОДПУ №242/96 було затверджено Положення про спеціальні відділення при Повноважних представництвах (далі – ПП) ОДПУ. Ці відділення виконували такі завдання:

– організовували секретне та шифрувальне діловодство у всіх установах, розташованих на території ПП ОДПУ як місцевого, так і союзного значення;

– здійснювали контроль за порядком ведення і зберігання мобілізаційних і шифрувальних матеріалів;

– вели облік осіб, що відали секретним листуванням в радянських установах;

– виробляли шифри і забезпечували ними всі установи, розташовані на території повноважного представництва за винятком тих, які користувалися шифром, встановленим Спеціальним відділом ОГПУ.

У 1927 році шифрувальний відділ НКЗС, який складався з трьох підвідділів, був реорганізований у секретно-шифрувальний відділ у складі двох підвідділів. На базі 3-го підвідділу був утворений секретний архів НКЗС.

1 грудня 1929 року наказом ОДПУ №282 у складі ОДПУ, крім Спецвідділу, було утворене ще Центральне шифрувальне бюро (начальник – В.М.Колосов, він же – начальник 1 відділення Спецвідділу), яке відповідало за шифрований зв'язок.

У той час Спецвідділ складався з таких підрозділів:

– 1 відділення – спостереження за збереженням режиму секретності у всіх партійних, державних і громадських організаціях, начальник – В.М.Колосов;

– 2 відділення – створення шифрів і кодів для ОДПУ, НКВМС і НКЗС, радіоперехоплення, начальник – Федір Григорович Тіхоміров;

– 3 відділення – керівництво шифрувальною роботою в системі ОДПУ, зв'язок із закордонними резидентурами, а також керівництво таборами ОДПУ, начальник – Федір Іванович Ейхманс, він же помічник начальника Спецвідділу;

– 4 відділення – дешифрування перехоплених документів, начальник -Олександр Григорович Гусєв (з вересня 1923 по січень 1938 року), він же – помічник начальника Спецвідділу;

– 5 відділення – криптографічне обслуговування військового відомства, начальник – Володимир Дмитрович Цибізов;

– лабораторія (що у свій час іменувалася 7-м відділенням і займалася прикладною хімією і графологією, начальник – Євген Євгенович Гоппіус;

– технічне відділення, начальник – Антон Дмитрович Чурган;

– фотографічне, начальник – П. Алексєєв.

Коло питань, що вивчалися підрозділами, які працювали на лабораторію Гопіуса, було надзвичайно широким: від винаходів усіляких пристосувань, пов'язаних із радіошпіонажем до дослідження сонячної активності, земного магнетизму й проведення різних наукових експедицій. Отут вивчалося все, що мало будь-який відтінок таємничості.

Контроль технічних нововведень радянської криптослужби здійснював заступник начальника її оперативного відділу Ейхманс. Всі фахівці-криптологи та радіотехніки прохо-

дили за таємним позаштатним розкладом. Загальна кількість особового складу Спецвідділу складала 189 осіб.

Цікаво, що начальник Спецвідділу Бокій робив спроби використовувати для криптологічної діяльності фахівців з окультних та містичних наук. Так, взимку 1924 року він залучив до роботи на Спецвідділ вченого-містика Олександра Барченка. Основні наукові інтереси цього дослідника були зосереджені в сфері вивчення біоелектричних явищ в житті клітини, в роботі мозку та живому організмі в цілому. Свої лабораторні досліди Барченко суміщав з посадою експерта Спецвідділу з психології та парапсихології. Зокрема, ним розроблялася методика виявлення осіб, схильних до криптологічної роботи та розшифровування кодів.

Вчений виступав і консультантом при обстеженні всіляких знахарів, шаманів, медіумів, гіпнотизерів і інших людей, які стверджували, що вони спілкуються з примарами. З кінця 1920-х років Спецвідділ активно використовував їх у своїй роботі. Для перевірки цих «екстрасенсів» один із підрозділів служби Бокія обладнав «чорну кімнату» в будівлі ОДПУ за адресою: Фуркасівський провулок, будинок 1.

Дослідження та методика Барченка застосовувалися і в особливо складних випадках дешифрування ворожих повідомлень – в таких ситуаціях проводилися навіть групові сеанси зв'язку з духами.

Барченко привніс в життя Бокія метафізичні теорії та умовив видного чекіста вступити в таємну окультну організацію «Єдине Трудове Братерство», що вивчала стародавню науку «Дюнхор», яка нібито перевершувала сучасне знання, але принципи якої були втрачені з часом.

До складу «Єдиного Трудового Братерства» увійшли, крім Бокія, ще такі особи: член ЦК ВКП (б) Моськвін, заступник наркома закордонних справ Стомоняков, працівник Спецвідділу Гоппіус, а також давні товариші Бокія по Гірському інституту інженери Міронов і Кострікін. Крім того, відомо, що на доповідях Барченка про «Дюнхор» були присутні в різний час співробітники Спецвідділу Гусєв, Цибізов, Філіпов і Леонов.

У кінці 1925 року для передачі езотеричного знання найбільш «гідним» представникам більшовицької партії Олександр Барченко за участю Бокія організував у «надрах» ОДПУ невеликий гурток із вивчення «Дюнхору». До нього увійшли провідні співробітники Спецвідділу: Гусєв, Цибізов, Кліменков, Філіпов, Леонов, Гоппіус, Плужніцов. Заняття із співробітниками Спецвідділу продовжувалися недовго, оскільки, за словами самого Бокія, учні виявилися «не підготовленими до сприйняття таємниць стародавньої науки». Врешті-решт, гурток Барченка розпався, але декілька разів його заняття відвідував і Генріх Ягода – майбутній шеф НКВС.

28 березня 1928 року на нараді у начальника 2-го відділу Управління справами НКВМС і РВР СРСР було прийнято ухвалу про організацію «військово-морської частини з дешифрування в Центрі, у Москві». Але справа просувалася украй поволі. Нова нарада, що відбулася 10 січня 1929 року та була присвячена тому ж питанню, на якому крім керівників ОДПУ і Спецвідділу, представників штабу РСЧА і Військово-морського флоту були також працівники морських штабів Балтійського та Чорного Морів, знов підтвердила необхідність організації відповідної дешифрувальної служби. Проте пройшов ще рік, а «військово-морська частина з дешифрування» ще не була створена.

Наприкінці лютого 1930 року Бокій підготував листа Ворошилову, в якому писав: «Спеціальний відділ при ОДПУ вважає такий темп, узятий штабом РСЧА у вирішенні питання щодо організації військово-морської частини з дешифрування, дуже повільним. Бажано прискорити вирішення цього питання, тобто стосовно дешифрувальної служби РСЧА відстала від армій своїх можливих супротивників, у яких ця справа давно налагоджена».

І лише у серпні 1930 року був створений перший дешифрувальний підрозділ при штабі РСЧА. Знаходився він у оперативному підпорядкуванні Спецвідділу при ОДПУ і фактично

входив у його склад. За штатом він іменувався 13-м сектором 7-го відділу Штабу РСЧА. Наказом РВР від 5 серпня 1930 року було затверджене «Положення про 7-й відділ».

В одному з пунктів цього Положення було записано, що на відділ покладалися питання організації дешифрувальної роботи, керівництво та контроль над нею. «Начальник 7-го відділу в спеціальному відношенні підпорядковується начальнику Спеціального відділу при ОДПУ». Начальником військово-морського дешифрувального сектора було вирішено призначити помічника начальника Спецвідділу при ОДПУ Павла Хрисанфовича Харкевича.

Розвиток військової дешифрувальної служби просувався швидкими темпами. Менш ніж через рік 13-й дешифрувальний сектор був реорганізований у 5-й відділ 4-го управління штабу РСЧА, але як і раніше залишився в оперативному підпорядкуванні Спецвідділу при ОДПУ. Всі працівники відділу мали хорошу мовну підготовку та зарекомендували себе здібними аналітиками. Провідними фахівцями у дешифруванні військових шифрів того часу були Борис Володимирович Звонарьов, Карл Густавович Тракман, Павло Матвійович Шунгський тощо.

15 листопада 1929 року були відкриті «Курси вдосконалення командного складу РСЧА», на яких готувалися офіцерські кадри шифрувальної служби. Тоді ж у Херсоні в найсуворішій таємності був організований відділ з підготовки офіцерів шифрувальної справи. Саме випускники херсонського відділу згодом брали участь у розробці малогабаритної дискової кодувальної машини К-37 «Кристал», що зробила дійсну революцію в шифрувальній справі.

У січні 1931 року були відкриті об'єднані дешифрувально-розвідувальні 3-місячні курси «спецпризначення» для підготовки криптологів дипломатичного та військового напрямів. Начальником курсів був призначений Харкевіч, а викладачами – Зибін, Ямченко, Аронський, Кильдишев. У 1934 році начальником цих курсів був призначений досвідчений криптолог Сергій Григорович Андреєв, який працював у Спецвідділі з 1921 року.

12 лютого 1930 року адміністративна комісія НКЗС розглянула питання про покращення роботи й зміну структури секретаріату колегії та ухвалила виділити зі складу секретаріату секретно-шифрувальний відділ як самостійний відділ та підпорядкувати його безпосередньо одному з членів колегії. 3 березня 1930 року Колегія НКЗС СРСР затвердила це рішення комісії.

У березні 1930 року начальником 1-ої (шифрувальної) частини IV (Розвідувального) Управління Штабу РСЧА був призначений Озолін, а дешифрувальний сектор 8-го відділу Штаба РСЧА був переведений до 5-го відділення Спецвідділу при ОДПУ для забезпечення спільної роботи над шифролистуванням іноземних держав.

У вересні 1930 року 2-й відділ Управління справами НКВМС був реорганізований у 7-ий відділ Штабу РСЧА, а вже 13 жовтня 1930 року – у 8-й відділ Штабу РСЧА. У штабах військових округів і морів шифроргани іменувалися 7-ми відділами, які у лютому 1931 року були перейменовані в військових округах у 8-і відділи, а на морях і флотах – 10-і відділи.

У березні 1931 року у складі IV Управління (з 22 листопада 1934 року – 5 Управління) Штабу РСЧА був утворений 5-й (дешифрувальний) відділ (начальник – Харкевич). Військово-дешифрувальний сектор 5-го відділення Спецвідділу при ОДПУ був переведений до 5-го відділу IV управління Штабу РСЧА.

У зв'язку із збільшенням обсягу та підвищенням значення дешифрувальної роботи у 1932—1933 роках були створені дешифрувальні групи при повноважних представництвах ОДПУ у Києві, Тбілісі, Хабаровську, Ташкенті і Ленінграді, а потім у Читі і Владивостоку. Пізніше ці групи були перетворені у дешифрувальні відділення.

У 1931—1932 роках криптовідділи були утворені вже у всіх військових округах, а до середини 30-х років чисельність криптослужб СРСР у центрі й на місцях досягла приблизно 500 осіб, що цілком відповідало потребам того часу. Склалася досить ефективна система криптослужб, які дешифровували до 30% всієї перехопленої інформації, що було дуже гарним показником для того часу.

У 1932 році було утворене дешифрувальне відділення в Особливій Далекосхідній Армії, а у 1935—1936 роках – у Забайкальському, Середньоазіатському та Київському військових округах. Ці відділення, так само як і в центрі, знаходилися в оперативному підпорядкуванні ОДПУ.

7 червня 1934 року начальник IV Управління (розвідувального) Штабу РСЧА Берзін, куди входила у той час військова дешифрувальна служба, представив наркому з військово-морських справ, голові РВР маршалу Ворошилову доповідь про дешифрувально-розвідувальну службу (ДРС):

«Шифродокументи поступають від 52 країн, проте розробляються спільно із Спеціальним відділом при ОДПУ як тільки документи 22 країн… За 1933 р. при напруженій роботі часом за рахунок передчасного зносу розумових та фізичних сил працівників ДРС розроблено тільки 42% матеріалів, що є для розробки. 58% іноземних шифрованих документів, що можуть дати цінну додаткову інформацію, залишилися необробленими через нестачу кадрів».

У доповіді було висловлено прохання про посилення служби кадрами, зокрема пропонувалося збільшити чисельність кадрового складу на 10 чоловік і перевести 16 чоловік вільнонайманих у адміністративний склад. Не зважаючи на скромність прохань, викладених у доповіді Берзіна, вони не були у 1934 році задоволені, тому відділ продовжував працювати в колишньому чисельному складі.

У 1933 році шифрувальники Спецвідділу при ОДПУ працювали у великій кімнаті на 4-му поверсі обширної будівлі колишньої страхової компанії на вулиці *«Лубянка»* в Москві. А дешифрувальники займали верхній поверх колишньої будівлі НКЗС на розі вулиць *«Лубянка»* і *«Кузнецкий мост»*. Той факт, що нижні поверхи будівлі відвідувалися приватними особами і членами дипломатичного клубу, використовувався для маскування.

10 липня 1934 року ОДПУ увійшло до складу НКВС як Головне управління державної безпеки (далі – ГУДБ), а його регіональні органи увійшли до складу регіональних управлінь НКВС. Згідно з цим Спецвідділ ОДПУ був реорганізований у Спецвідділ ГУДБ НКВС.

22 листопада 1934 року було оголошено Ухвалу ЦВК і РНК СРСР про затвердження Положення про Народний комісаріат оборони (далі – НКО), згідно з яким у його склад увійшло Розвідувальне управління (далі – РУ), що раніше входило до складу штабу РСЧА. 15 грудня 1935 року був змінений і затверджений новий штат РУ РСЧА, згідно з яким 5-ий (дешифрувальний) відділ став 7-м відділом, а 1-а (шифрувальна) частина стала таємно-шифрувальним відділенням (іноді іменувалося відділенням «Ш»). Чисельність 7-го відділу складала 53 особи і 5 осіб постійного складу було виділено на Центральні курси ДРС.

Начальником 7-го відділу з лютого 1936 року по лютий 1939 року був полковник Харкевич, а його заступником – майор Звонарьов, який досконало володів чотирма іноземними мовами, трьома європейськими і японською. Начальником відділення «Ш» з січня 1935 року по листопад 1937 року був полковий комісар Озолін, а з вересеня 1938 року по травень 1939 року – майор Микола Олександрович Філатов.

У 1935 році за виконання спеціального завдання командування Звонарьов був нагороджений іменним золотим годинником наркома оборони, а у 1936 році – орденом Червоного Прапора. Річ у тому, що фахівці ДРС спільно з фахівцями Спецвідділу розкрили у жовтні 1935 року японський дипломатичний код, про що доповіли начальнику Розвідувального управління РСЧА С.Г.Урицькому. Останній написав рапорт заступнику наркома Гамарнику, а він, враховуючи важливість події, розпорядився доповісти про це особисто наркому Ворошилову. Ось доповідь Урицького Ворошилову:

«15 жовтня п. р. японський уряд відхилив свій основний код і ввів замість нього новий. Виникла загроза не мати інформації про військові заходи Японії щодо лінії дешифрування японських шифротелеграм у потрібний момент. Помічник начальника… відділу РУ РСЧА т. Звонарьов Б. В. спільно з працівниками його підрозділу тт. Шунгським, Калініним, Мильни-

ковим і працівниками Спецвідділу ГУДБ НКВС тт. Єрмолаєвим і Єрмаковою у мінімально короткий термін, у 6 днів, розкрили вказаний код і забезпечили безперебійне розшифрування японських шифротелеграм. Ці результати досягнуті завдяки систематичній підготовці т. Звонарьовим свого підрозділу до виконання завдань, що стоять перед ним. Безпосередньо при розкритті коду особливо важливу роль зіграли тт. Звонарьов і Шунгський. Клопочу про нагородження цінними подарунками… т. Звонарьова Б. В. і фахівців тт. Шунгського, Калініна і Мильникова…»

На цьому рапорті нарком оборони наклав резолюцію: «Нагородити т. Звонарьова золотим годинником, а решту тт. срібними (хорошими) годинниками. К.В. 27.XI.35 р.».

У 1935 році шифрувальники та дешифрувальники Спецвідділу переїхали в нову будівлю на вулиці імені Фелікса Дзержинського. Шифрувальний відділ був розділений на декілька відділень, які займалися забезпеченням секретного зв'язку з регіональними управліннями секретної поліції, з її прикордонними частинами і військовими формуваннями, з адміністраціями в'язниць і таборів, з нелегальною закордонною агентурою і з «легальними» резидентурами за кордоном.

За секретний зв'язок з «легальними» резидентурами відповідало 6-е відділення. Його начальник з прізвищем Козлов був знятий з посади під час репресій у 1937 році. А після того, як наступник Козлова був відправлений шифрувальником до США, начальником 6-го відділення стала людина, чиє ім'я придбало згодом скандальну популярність. Це був Володимир Петров, який у 1954 році разом з дружиною Євдокією отримав політичний притулок в Австралії.

Дешифрувальний відділ був розділений на відділення за географічним і мовним принципом – китайське, японське, англо-американське і так далі. Майбутня пані Євдокія Петрова (Дуся), яка протягом двох років вивчала японську мову в московській спецшколі, працювала в японському відділенні. її колегами по роботі були:

– Віра Плотнікова, дочка професора японської мови, яка протягом багатьох років була резидентом японської розвідки у Москві;

– Галина Підпалова, настільки закохана у все японське, що, прийшовши додому, вона незмінно одягалася в кімоно;

– Іван Калінін, який час від часу запрошувався як консультант;

– професор Шунгський – головний авторитет відділення з питань японської мови, який служив ще в царській армії.

У 1938 році була проведена чергова реорганізація НКВС. В результаті для ведення шифрованого листування у його структурі 9 червня був утворений 3-й спецвідділ, начальником якого став капітан держбезпеки Олександр Дмитрович Баламутов. 29 вересня Спецвідділ ГУДБ НКВС був перейменований у 7-й відділ начальником якого став той же Баламутов. У 1939 році до складу 7-го відділу ГУДБ НКВС було переведене дешифрувальне відділення Розвідувального відділу НКВМФ СРСР, яке було утворене у 1938 році. 9 квітня 1939 року начальником 7-го відділу був призначений капітан держбезпеки Олексій Іванович Копитцев. Станом на 1 січня 1940 року у складі 7-го відділу працювало 230 осіб.

У травні 1939 року був реорганізований і секретно-шифрувальний відділ НКЗС. Шифрувальний відділ був виділений з нього як самостійний відділ з безпосереднім підпорядкуванням заступнику наркома та перейменований у 10-й відділ НКЗС. Найменування посади «шифрувальник» було скасовано та були введені посадові назви «референт», прийняті в оперативних відділах НКЗС.

19 липня 1939 року відповідно до Постанови Комітету Оборони СРСР 8-й відділ ГШ РСЧА був перейменований у Відділ шифрувальної служби і включений на правах самостійного структурного підрозділу до складу Оперативного управління ГШ РСЧА.

У 1939 році у зв'язку з реорганізацією 5-го (розвідувального) Управління НКО шифрувальне відділення стало 9-м відділом, а 7-й (дешифрувальний) відділ став 11-м відділом. Начальником 9-го відділу до жовтня 1939 року був Філатов, а з жовтня 1939 року став майор Леонтій Сергійович Пілєвін. Начальником 11-го відділу з жовтня 1939 року став Філатов.

Наказом НКО СРСР №0038 від 26 липня 1940 року 5-е (розвідувальне) Управління НКО увійшло до складу Генерального штабу (далі – ГШ) Червоної Армії (далі – ЧА) і почало називатися РУ ГШ ЧА. У його складі залишився 9-й (шифрувальний) відділ (начальник – майор Пілєвін), а 11-й (дешифрувальний) відділ став 10-м відділом (начальник – полковник Філатов). 18 серпня 1941 року на базі Відділу шифрувальної служби Оперативного управління ГШ ЧА було створено Управління шифрувальної служби ГШ ЧА загальною чисельністю 197 військовослужбовців і 50 службовців.

Указом Президії Верховної Ради (далі – ПВР) СРСР від 3 лютого 1941 року зі складу НКВС був виділений наркомат державної безпеки (далі – НКДБ). Шифрувально-дешифрувальна справа перейшла до 5-го відділу НКДБ, начальником якого став майор держбезпеки Копитцев. Для ведення шифролистування у складі НКВС наказом №00198 від 22 лютого 1941 року було організовано 6-е відділення, начальником якого став Солодянніков.

Після початку Вітчизняної війни Указом ПВР СРСР від 20 липня 1941 року НКВС і НКДБ були знов об'єднані в єдиний НКВС. Шифрувально-дешифрувальна справа перейшла до 5-го спецвідділу НКВС, начальником якого став майор держбезпеки Іван Григорович Шевельов, а його заступником – старший майор держбезпеки Копитцев. Спецвідділ станом на 20 травня 1942 року мав за штатом 683 одиниці та складався з 16 відділень, завдання яких були такими:

– 1—8 – дешифрувально-розвідувальна робота закордоном;

– 9 – складання, дослідження та друкування кодів для НКЗС, НКВТ, НКВС, НКО і НКВМФ;

– 10 – складання та друкування блокнотів для НКО, НКВМФ, НКВС, НКЗС, НКВТ;

– 11 – здійснення шифрозв'язку оперативно-чекістських управлінь і відділів НКВС; зашифрування та розшифрування телеграм, облік і постачання шифродокументів периферійним органам НКВС і їх інструктаж щодо шифроботи;

– 12 – здійснення шифрозв'язку таборів НКВС, прикордонних, внутрішніх і оперативних військ НКВС, Прокуратури, Військової колегії Верховного суду СРСР;

– 13 – здійснення шифрозв'язку закордонної резидентури 1-го Управління НКВС;

– 14 – оперативно-чекістське обслуговування шифрорганів наркоматів і інших установ;

– 15 – перевірка та допуск осіб, що працюють з секретними, мобілізаційними та шифрувальними документами в установах і підприємствах; спецперевірка особового складу, що працюють на особливо режимних підприємствах.

16 лютого 1942 року наказом НКО №0033 РУ ГШ ЧА було реорганізоване в Головне РУ (далі – ГРУ), а 23 вересня наказом НКО №00222 з метою концентрації зусиль щодо «розкриття» шифролистування супротивника дешифрувальна служба ГРУ була передана до 5-го спецвідділу НКВС. 3 листопада наказом НКВС №002424 на базі 5-го спецвідділу, до якого увійшли 7-й відділ (дешифрувальний) 2-го Управління ГРУ та частини спецслужби внутрішніх військ НКВС (радіорозвідка) було утворено 5-е Управління НКВС. Його начальником став старший майор держбезпеки Шевельов, а його заступником – комісар держбезпеки Копитцев.

Ще у квітні-травні 1941 року в криптослужбу НКВС було мобілізовано близько 50 молодих учених з Московського державного університету (далі – МДУ) – математиків і фізиків, а також випускників Військової академії зв'язку. Вони не тільки змогли швидко знайти в ній своє місце, але й привнесли в криптоаналітичну роботу нові ідеї. Якщо «старі» фахівці уміли копітко, крок за кроком накопичувати інформацію про ключ шифру супротивника, то математики, аналізуючи логіку побудови лише частково відомого ключа, знаходили алгоритми його

істотного поповнення. Інженери і фізики почали створювати та впроваджувати в аналіз шифрів допоміжну техніку. Ці два чинники сприяли здійсненню якісного стрибка в розкритті ключів вермахту, що часто мінялися.

У грудні 1942 року на базі Школи особливого призначення 5-го Управління НКВС і 3-го учбового відділення Вищої школи Генштабу була організована Спеціальна школа 5-го Управління НКВС у складі двох відділень з 10-місячним терміном навчання. Перше відділення цієї школи готувало кадри криптоаналітиків для дешифрування військового листування, а друге відділення – дипломатичного листування.

У роки Вітчизняної війни криптопідрозділи дешифрувальної служби поповнювалися в основному за рахунок тих, що закінчили Спеціальну школу 5-го Управління НКВС, в якій було підготовлено багато провідних фахівців. Отримувані в школі спеціальні і мовні знання дозволяли її випускникам швидко включатися в роботу з криптоаналізу та дешифрування. Спеціальна школа, а також ряд криптопідрозділів, що знаходилися в Уфі, підпорядковувалися Копитцеву. Частини спеціальної служби військ НКВС здійснювали ведення радіорозвідки. На них покладалися завдання розвідки ефіру, здійснення радіоперехоплення, шифрованого радіолистування, попередньої обробки цих даних з радіомереж і окремих радіоточок.

У складі 5-го Управління була також утворена Криптографічна Рада для організації і координації наукових досліджень і підготовки наукових кадрів у спецслужбі (за роки війни розглянула більше 60 питань і проблем за основними напрямами спеціальної роботи).

14 квітня 1943 року у зв'язку з наближенням радянських військ до кордонів СРСР рішенням Політбюро ЦК ВКП (б) № П 40/91 «Про утворення НКДБ СРСР» і ухвалою РНК СРСР №393—129сс зі складу НКВС знову був виділений НКДБ. Шифрувально-дешифрувальна справа та спецзв'язок перейшли до 5-го Управління НКДБ. Його начальником став комісар держбезпеки Шевельов, а його заступниками – комісар держбезпеки Копитцев і старший майор держбезпеки Сергій Вікторович Покотіло.

Для ведення шифролистування у складі НКВС наказом №00776 від 28 квітня 1943 року був утворений 2-й спецвідділ, начальником якого став підполковник держбезпеки А. Воробйов, а з 1944 року по 21 березня 1949 року був підполковник В. Романов. Станом на 1 квітня 1945 року спецвідділ мав по штату 52 одиниці, а в наявності – 49 осіб. 3 травня 1949 року наказом МВС №544 начальником спецвідділу був призначений колишній заступник начальника Управління кадрів МВС полковник І.І.Філаткін.

Закінчення Другої світової війни та зміни у світовому геополітичному становищі підштовхнула радянський уряд до реорганізації органів влади та державної безпеки. Так, 15 березня 1946 року 5-а сесія Верховної Ради СРСР прийняла Закон про перетворення Ради Народних Комісарів СРСР в Раду Міністрів СРСР, а народних комісаріатів – у міністерства.

Таким чином, НКВС перетворився у МВС, НКДБ – МДБ, НКЗС – МЗС, НКО – МО тощо. Наказом НКДБ №00107 від 22 березня 1946 року 5-е (шифрувально-дешифрувальне) Управління НКДБ стало 6-м Управлінням МДБ. Його начальником став генерал-лейтенант Шевельов, а його заступником – генерал-майор Копитцев.

20 серпня 1946 року Рішенням Політбюро ВКП (б) була затверджена нова концепція структури держбезпеки та її напрямків діяльності. Вона припускала подальший розподіл органів держбезпеки та створення незалежних та конкуруючих між собою спецслужб, причому Секретаріат ЦК ВКП (б) виступав у цій схемі як арбітр. На виконання даної концепції у травні 1947 року на базі 1-го ГУ МДБ і ГРУ ГШ ЗС було утворене нове розвідувальне відомство – Комітет Інформації при Раді Міністрів СРСР, який проіснував до 1951 року. До його складу увійшов і дешифрувальний відділ ГРУ ГШ ЗС, який був реорганізований у 7-е Управління Комітету Інформації.

19 жовтня 1949 року Постановою Політбюро ЦК ВКП (б) № П71/426 було прийнято найважливіше для радянської криптології рішення. Вся шифрувально-де-шифрувальна робота

з МДБ передавалася до ЦК ВКП (б) і, відповідно, 6-е Управління МДБ ліквідовувалось. Це було оформлено наказом МДБ №00369 від 15 листопада, а у складі ЦК ВКП (б) було створено Головне управління спеціальної служби (далі – ГУСС). Його начальником став генерал-лейтенант Шевельов, а начальником 1-го Управління (дешифрувально-інформаційного) – генерал-майор Копитцев.

4. Утворення радянської шифротехніки

В даний час у закордонній і вітчизняній літературі є багато публікацій про закордонні електромеханічні шифрувальні машини, аж до описів принципів їхніх дій і фотографій. При цьому аналогічних публікацій про радянську шифрувальну техніку (також застарілої і знятої з експлуатації) дотепер дуже мало. Недостатність інформації з цього питання створює помилкове враження, що шифрувальна справа в СРСР у частині автоматизації найскладних процесів шифрування безнадійно відстала від передових країн світу. Але насправді це не відповідає дійсності.

Більш того, існуючий пробіл в історії вітчизняного спеціального приладобудування, як частини історії країни, незаслужено збіднює її в цілому, тому що створення у 1930-і роки в Ленінграді вітчизняної шифрувальної техніки та організація її промислового виробництва є досягненнями національного рівня. Це варто знати та пишатися нашими попередниками. Крім того, власний шлях еволюційного розвитку вітчизняних шифрувальних машин також являє історичну цінність, особливо в порівнянні з досягненнями передових у цій сфері західних країн того часу.

У молодій Радянській республіці ніякої шифрувальної техніки не існувало зовсім, але багато хто вже серйозно задумувалися над тим, як вирішити цю проблему. Саму активну позицію з цього питання займали фахівці 8-го (криптологічного) відділу ГШ РСЧА. Однак перша спроба створити електромеханічний шифратор була розпочата не криптологами та не шифрувальниками. Є дані, що це зробили в 1923 році фахівці Особливого технічного бюро з військових винаходів спеціального призначення (далі – ОТБ), що не мали до шифрувальної справи ніякого відношення.

ОТБ було утворене 18 червня 1921 року Постановою Ради Праці й Оборони як філія московського науково-дослідного інституту (далі – НДІ) №20, що займався розробками в сфері радіотехніки для армії і флоту. Очолив нове відомство талановитий російський винахідник В. Бекаурі.

В ті роки радянському керівництву вже стало зрозуміло, що наявні ручні системи й способи шифрування й кодування, скільки б їх не вдосконалювали й модернізували, не в змозі впоратися із все зростаючими потоками інформації в силу слабкої швидкості її обробки. Було загострено питання щодо механізації даного процесу.

У 1923 році в ОТБ був розроблений і, навіть, виготовлений діючий макет дискового шифратора. Більш докладні дані про нього відсутні, та й подальша розробка шифратора була припинена, тому що це відволікало фахівців від планової роботи термінового характеру. Після масових репресій 1937—1938 років в ОТБ та його наступної реорганізації зник і сам шифратор. Він, можливо, був просто знищений як не потрібний для людей, далеких від проблем криптології. Проте можна констатувати, що одна з перших спроб механізувати процес шифрування в Радянській республіці усе-таки відбулася.

Наступна спроба ініціювати розгляд питання щодо створення вітчизняної шифрувальної машини була розпочата шифрувальниками-моряками на нараді у 2-му відділі Управління справами Народного комісаріату з військових і морських справ, що відбулася в січні 1929 року. До порядку денного серед інших було включене питання про «машинізацію» шифрування (термінологія того часу), ретельно підготовлений морськими шифрувальниками. У результаті детального обговорення було докладно з'ясоване, яку саме моряки хотіли б бачити першу шифрувальну машину. Підсумки наради занесли до протоколу, наприкінці якого потенційним розробникам запропонували заглянути у майбутнє: «…Вважати бажаним і найбільш прийнятним для кораблів флоту введення такої шифрувальної машини, що одночасно самошифрує і пере-

дає радіоапара-том…». Показово, що вже в 1929 році радянські моряки порушили питання про створення не просто машини попереднього шифрування, а машини лінійного шифрування.

Конец ознакомительного фрагмента.