История создания и становления Агенства безопасности связи Армии США (1914-1945 гг.)

Первая мировая

К началу Первой мировой войны задачи обеспечения безопасности связи и криптографической защиты сообщений в американской армии были возложены на три ведомства. Управление военной разведки отвечало за разработку армейских кодов и шифров, специальное подразделение генерал-адъютантской службы обеспечивало изготовление кодовых книг и шифрдокументов и их рассылку в подразделения, а на войска связи была возложена ответственность за эксплуатацию шифровальной аппаратуры и ее поставку в подразделения армии.   
Подготовка специалистов по криптоанализу для армии США была начата за несколько лет до начала Первой мировой войны и первоначально осуществлялась в школе войск связи, расположенной в Форт-Ливенворт. Позднее все вопросы, связанные с подготовкой таких специалистов, были переданы в ведение Управления военной разведки. Подготовка офицерского и рядового состава стала осуществляться во вновь созданной армейской школе криптологии, которая разместилась в местечке Ривербэнк, недалеко от г. Женева, штат Иллинойс. Руководство школой было возложено на известного специалиста в области криптологии полковника Джорджа Фабиана, которому удалось привлечь к преподаванию в школе ряд гражданских профессоров и ученых. Среди них был и Уильям Фридман, в последующем один из руководителей и ведущих специалистов армейской дешифровальной службы.  
6 апреля 1917 г. американский Конгресс объявил о вступлении США в войну с Германией. Для участия в боевых действиях на территорию Франции было переброшено морем экспедиционное соединение американских войск под командованием генерала Джона Першинга численностью более 175 тыс. человек. На его подчиненного, начальника связи экспедиционного соединения бригадного генерала Эдгара Рассела, были возложены задачи по организации надежной и безопасной связи частей соединения, разработке и рассылке кодовых книг и шифрдокументов, а также руководство подразделениями радиоразведки по добыванию сведений о противнике.  
Чтобы исключить чтение противником передаваемых по средствам радиосвязи важных сообщений, экспедиционным соединением достаточно широко использовались различные коды и шифры - военный телеграфный код, шифр с бегущим ключом (использовался в механическом шифрующем устройстве роторного типа), а также английский шифр "Плэйфер". Однако, как выяснилось впоследствии, все они обладали низкой криптоустойчивостью и не обеспечивали надежной защиты сообщений от разведки противника.  
Подчиненное бригадному генералу Расселу небольшое по численности специальное подразделение занималось составлением полевых кодов. Оформленные в виде таблиц коды предназначались для преобразования открытых текстов команд, распоряжений и донесений в эквивалентные им условные группы буквенно-цифровых символов. Рассылаемые в подразделения кодовые книги имели малый формат, были удобны для использования в полевых условиях и содержали около 30 000 слов (фраз) и соответствующих им кодовых значений.   
Работа подразделения была достаточно сложной, особенно в случае компроментации кода. Один из таких случаев произошел с кодом под названием "Потомак", который попал в руки немцев через месяц после поступления кодовых книг в подразделения экспедиционного соединения американских войск. Потребовалось около двух суток напряженной работы личного состава подразделения для его полной замены. Всего за 10 месяцев боевых действий подразделением было составлено, отпечатано и разослано в войска более 80 000 кодовых книг.  
Характерной чертой Первой мировой войны, помимо применения воюющими сторонами новых видов вооружения - самолетов, танков, подводных лодок, стало появление нового вида военной разведки - радиоразведки. Ее успеху и широкому развитию способствовали интенсивное применение средств радиосвязи, многочисленные нарушения радистами правил радиообмена, передача по радио секретных распоряжений и приказов, зашифрованных с использованием несложных кодов и шифров. Наряду с русской, английской, французской, германской и австро-венгерской армиями радиоразведка в годы Первой мировой войны велась и подразделениями экспедиционного соединения американских войск. Посты подслушивания, в состав которых входили подготовленные военнослужащие, владеющие немецким языком, размещались в непосредственной близости от районов расположения немецких войск. Подключив телефонные аппараты к проводным линиям связи противника, они осуществляли прослушивание и запись передаваемых по ним телеграфных и телефонных сообщений. Посты радиоперехвата, расположенные, как правило, на значительном удалении от линии фронта, позволяли без непосредственного соприкосновения с противником добывать ценные сведения о его группировке, действиях и намерениях. Возможности американской радиоразведки существенно повышались благодаря использованию постов радиопеленгования, определявших местоположение войсковых радиостанций противника.  
Зашифрованные сообщения противника с постов подслушивания и радиоперехвата поступали в отдел военной разведки экспедиционного соединения, где специалисты по дешифрованию пытались вскрыть используемые немецкими войсками коды и шифры. Криптоаналитической работой в отделе в основном занимались выпускники и бывшие преподаватели армейской криптологической школы (в их числе был и У. Фридман), которые были призваны на военную службу после вступления США в войну с Германией.

Создание Службы радиоразведки

В 1921 году обязанности по разработке армейских кодов и шифров были переданы из Управления военной разведки в Управление начальника войск связи. В составе последнего была создана Секция кодов и шифров, первым руководителем которой (в качестве гражданского служащего) стал У. Фридман. Основной задачей, возложенной на новое подразделение, стала разработка кодов, а также средств и методов криптографической защиты сообщений в армейских системах связи. В 1922 г. в результате предпринятых Секцией усилий на вооружение американской армии начинает поступать малогабаритное шифровальное устройство роторного типа М-94, которое было предназначено для использования в полевых условиях и шло на замену устаревшего образца, находящегося на вооружении армейских частей уже много лет. Для оценки криптостойкости нового шифра специалистам по криптоанализу было предоставлено 25 сообщений, зашифрованных с использованием одного и того же ключа. Несмотря на продолжительные попытки, взломать шифр не удалось. В последующие годы устройство М-94 широко использовалось для шифрования информации, передаваемой в тактическом звене связи, в частности при ведении боевых действий подразделениями американских войск в Китае и Бирме, вплоть до середины Второй мировой войны.   
Криптоаналитическая работа американской армии в 20-х годах была сосредоточена в так называемом "черном кабинете", созданном еще в 1917 г. Деятельность кабинета, которым руководил Герберт О. Ярдли, осуществлялась в обстановке строгой секретности и была направлена на вскрытие военных и дипломатических шифров зарубежных стран в интересах Военного министерства и Государственного департамента США. За время существования "черного кабинета" с 1917 по 1929 гг. им было дешифровано более 10 000 телеграмм европейских и южно-американских государств.   
Самым крупным успехом в его деятельности было вскрытие японских дипломатических кодов и шифров. В 1929 г. Генри Стимсон, будучи в то время Государственным секретарем США, перестал по этическим соображениям пользоваться услугами "черного кабинета" и выделять деньги на его содержание. В связи со сложившейся ситуацией в том же году на базе Секции кодов и шифров в составе Управления начальника войск связи была создана Служба радиоразведки (Signal Intelligence Service) во главе со все тем же У. Фридманом. Новой службе вменялись обязанности по разработке армейских кодов и шифров, перехвату сообщений, передаваемых по радио- и проводным линиям связи противника, пеленгованию его радиостанций, криптоанализу кодов и шифров и, наконец, лабораторные исследования в области тайнописи. Часть из указанных функций предполагалось выполнять только в случае ведения армией боевых действий.  
До начала Второй мировой войны Служба радиоразведки насчитывала всего 7 сотрудников. Несмотря на свою малочисленность, в 30-х годах ей удалось выполнить большой объем работ в области совершенствования армейских кодов и шифров, подготовки специалистов и создания новой аппаратуры шифрования и радиоразведки. В августе 1934 г. ей были переданы функции изготовления и рассылки кодовых книг и шифрдокументов, в результате чего все вопросы, связанные с криптографической защитой сообщений, оказались в ведении Управления начальника войск связи армии США.   
В конце 30-х годов Служба приобрела и испытала доставленные из Европы 50 коммерческих образцов малогабаритной шифровальной машины Хэйглина. В результате выполненной доработки на вооружение американской армии был принят усовершенствованный вариант -шифровальная машина М-209, которая стала использоваться в войсковых подразделениях от дивизии до батальона, поскольку обеспечивала лишь средний уровень криптостойкости. При участии специалистов Службы была также создана шифровальная машина М-134 - одна из наиболее совершенных по тому времени. Машина поступала на вооружение не только армии, но и Военно-морских сил США, которые принимали участие в финансировании работ по ее созданию.   
К моменту вступления Соединенных Штатов в войну с Японией М-134 была установлена в штабах всех основных частей и соединений Армии и ВМС и использовалась также на линии правительственной связи под условным наименованием POTUS-PRIMER (President of the United States - Prime Minister) для обеспечения зашифрованной связью Президента США с премьер-министром Великобритании.

Первые результаты деятельности подразделений радиоперехвата и криптоанализа

С 1934 г. в США действовал 605-й раздел Закона о федеральных средствах связи, в соответствии с которым подслушивание телефонных разговоров и перехват переписки между иностранными государствами и их дипломатическими представительствами в Америке были запрещены. Генерал Крейг, начальник штаба армии США с 1937 по 1939 гг., требовал от своих подчиненных неукоснительного выполнения этого закона, что сильно сдерживало создание подразделений радиоразведки. В 1939 г. Крейга сменил генерал Д. Маршалл, который считал Закон о федеральных средствах связи юридическим недоразумением.   
В связи с этим войсковые подразделения радиоразведки появились в США только в 1938 г. - именно тогда была создана 1 рота в Форт- Монмаут, а также образованы отдельные подразделения при пяти ротах связи, расположенных в Панаме, на Гавайских островах, Филиппинах, в штате Техас и районе Сан-Франциско. В 1939 г. в целях совершенствования управления созданными подразделениями на их базе в Форт-Монмаут была сформирована 2-я рота радиоразведки в составе 101 военнослужащего рядового состава и одного офицера - командира роты. Для зачисления на службу в роту военнослужащие проходили строгий профессиональный и морально-психологический отбор, преимуществом пользовались те из них, кто прослужил на военной службе определенный срок и выразил согласие на прохождение дальнейшей службы на военных базах США, дислоцированных за границей.  
Перед началом Второй мировой войны рота располагала шестью постами радиоперехвата: № 1 - Форт-Хэнкок, штат Нью-Джерси; № 2 - Сан-Франциско; № 3 - Форт-Шафтер, Гавайские острова; № 6 - Форт-Миллс, Манила, Филиппины; № 7 - Форт-Хант, штат Вирджиния; № 9 - Рио-де-Жанейро. Перехваченные постами шифртелеграммы направлялись для их криптоанализа в Службу радиоразведки, специалисты которой размещались в здании Военного министерства в Вашингтоне.   
Первоначально доставка материалов радиоперехвата в Вашингтон осуществлялась авиапочтой или морем, поэтому часто в связи с плохими погодными условиями происходили значительные задержки в отправке материалов. Для исправления ситуации перехваченные и предварительно зашифрованные американским военным шифром сообщения стали передаваться в столицу по каналам радиосвязи.   
В конце 30-х годов американской разведке в результате успешно проведенной операции удалось проникнуть в секреты построения новой японской шифровальной машины, которую специальные курьеры тайно перевозили морем из Токио в свое посольство в США. После тщательного изучения предоставленных в их распоряжение чертежей и других материалов группе армейских криптоаналитиков во главе с У. Фридманом удалось изготовить несколько копий японской шифрмашины. Одна из них была передана в Военно-морские силы США, а остальные остались в распоряжении армии. В августе 1940 г., после более чем полутора лет напряженной работы, Службе радиоразведки удалось вскрыть ряд японских дипломатических кодов и шифров, что позволило американскому военно-политическому руководству быть в курсе всей секретной радиопереписки Министерства иностранных дел Японии с его посольством в США.  
Поток сообщений японского МИД, перехватываемых подразделениями армейской и флотской радиоразведок, был достаточно велик, осенью 1941 г. он составлял от 50 до 75 радиограмм в сутки, при этом объем отдельных сообщений достигал 15 страниц отпечатанного текста. В связи с большой загрузкой специалистов по дешифрованию и с целью упорядочения их работы командованием армии и ВМС США было принято решение, согласно которому дешифрование сообщений, принятых по четным дням месяца, осуществлялось криптоаналитиками Армии, а по нечетным дням - криптоаналитиками ВМС.   
Работа подразделений радиоперехвата и криптоанализа накануне вступления США в войну с Японией была достаточно напряженной. Из 227 сообщений по вопросам японо-американских отношений, которыми обменялись МИД Японии и его посольство в Вашингтоне в период с марта по декабрь 1941 г., американской радиоразведке удалось перехватить 223 сообщения и только 4 радиограммы были пропущены.

Вторая мировая

Со вступлением США в декабре 1941 г. во Вторую мировую войну объем работы Службы радиоразведки стремительно возрастал. Ее численность за предшествующие два года увеличилась с 19 до 181 человека и продолжала расти, в связи с чем в августе 1942 г. личный состав Службы перебрался из Вашингтона в Арлингтон-Холл - просторное здание бывшей частной школы, расположенное в одном из пригородов штата Вирджиния на побережье реки Потомак.   
Практически одновременно с переездом в Управлении начальника войск связи армии США произошли организационные перемены - Служба радиоразведки была преобразована в Службу безопасности связи (Signal Security Service). В ее состав вошли батальон радиоразведки, школа радиоразведки и криптологии и 4 секции, каждой из которых было присвоено буквенное обозначение: А - административная, В - радиоразведки и криптоанализа, С - безопасности связи и криптографии, D -- тайнописи.  
В августе 1942 г. в целях координации деятельности полевых постов радиоперехвата в составе Службы была сформирована секция Е, а в декабре того же года - секция F, основным назначением которой стала организация работ по созданию новой шифровальной аппаратуры для Армии США.  
В середине 1943 г. после соответствующего увеличения численности личного состава все секции были переименованы в отделы, а Служба преобразована в агентство безопасности связи (Signal Security Agency).   
На протяжении всей войны наиболее многочисленным среди подразделений Службы был отдел В (радиоразведки и криптоанализа). Разведданные, подготовленные специалистами отдела на основании анализа перехваченных открытых и зашифрованных радиосообщений противника, направлялись в Управление военной разведки для их последующей оценки и использования. Высокая ценность докладываемых данных была обусловлена тем, что за годы войны американским криптоаналитикам удалось вскрыть ряд кодов и шифров противника: в 1942 г. ими был разгадан шифр ВМС Японии, а в 1943 г. были раскрыты и армейские японские шифры.  
Успеху отдела в немалой степени способствовало широкое применение его специалистами вычислительной техники - первоначально простых табуляторов, а впоследствии и более сложных, созданных на основе электронно-вакуумных ламп и логических схем, вычислительных машин типа RAM (Rapid Analytical Machine). Такая машина, благодаря ее высокому быстродействию, позволяла заменять ручной труд многих тысяч криптоаналитиков.  
В начале войны Служба располагала всего 13 простейшими машинами фирмы IBM, которые обслуживались 21 оператором из отдела А. Нехватка специалистов по криптоанализу на это время составляла около тысячи человек. Выход из создавшегося положения руководство Службы видело в более широком использовании при решении задач дешифрования средств вычислительной техники. Число используемых машин и обслуживающего персонала было увеличено, и летом 1944 г. в составе Агентства безопасности связи было создано новое подразделение - отдел G (вычислительной техники), который к весне 1945 г. располагал уже 407 машинами и насчитывал 1275 операторов. Численность отдела В, возглавляемого Соломоном Кульбаком, выросла к лету 1944 г. до 2574 человек, из них 82 % было сосредоточено на дешифровании сообщений японской армии. Общая численность агентства в это время (без учета личного состава подразделений 2-го батальона, проходившего службу за пределами территории США) составляла около 10 тыс. человек.   
Важным направлением в деятельности отделов В и G считалось также взаимодействие с Правительственной школой кодов и шифров Великобритании по дешифрованию сообщений немецких войск, которые использовали роторную шифровальную машину "Энигма". Взлом шифрованных сообщений "Энигмы" в первые годы войны проводился в Блетчли-Парк (уединенное поместье в 80 км севернее Лондона - местонахождения Правительственной школы кодов и шифров) и шел достаточно тяжело. Но после того как с 1942 г. английские криптоаналитики стали использовать несколько специализированных быстродействующих машин "Колосс", процесс дешифрования значительно ускорился.  
С появлением у американских специалистов вычислительных машин RAM, превосходивших по своему быстродействию английскую "Колосс", между Арлингтон-Холл и Блетчли-Парк был установлен специальный канал связи, по которому из Великобритании передавались перехваченные английской радиоразведкой шифровки "Энигмы". Только за период с июля 1943 по январь 1945 г. в Арлингтон-Холл поступило 1357 немецких шифровок, из которых 413 были успешно дешифрованы.  
В связи с широким применением всеми воюющими странами средств радиоразведки важным направлением деятельности Арлингтон-Холла являлось обеспечение безопасности связи частей и подразделений американских сухопутных войск. Решение указанной задачи достигалось за счет разработки совершенных кодов и шифров, создания новых образцов шифровальной аппаратуры, проведения мероприятий по радиомаскировке и контролю за соблюдением радиодисциплины операторами армейских радиостанций.  
Организация всех работ по созданию новой шифраппаратуры для Армии США была возложена на отдел F. Наряду с шифровальной машиной М-134 при участии специалистов отдела была разработана и более совершенная модель М-228 (SIGCUM), которая стала поступать в войска начиная с 1943 г. Машина представляла собой буквопечатающий аппарат, обеспечивающий шифрование набираемого на клавиатуре текста с одновременной передачей его в линию связи. Применение нового принципа действия позволило существенно повысить скорость передачи и приема шифрованных сообщений, что было весьма важно в связи со значительным ростом потоков информации в период проведения крупных военных операций. Так, в середине 1943 г. при проведении войсками союзников десантной операции по захвату острова Сицилия объем шифрованной радиопереписки штаба Пятой армии США достигал 23 тыс. кодовых групп в сутки, а в период Южно-итальянской операции - до 40 тыс. групп. Благодаря наличию шифрмашин М-228 штабу армии удавалось своевременно получать необходимую информацию от подчиненных частей, а также передавать им необходимые распоряжения, соблюдая при этом требования по скрытому управлению войсками.  
Наряду с рядом достоинств техническая конструкция машины имела и существенный недостаток - при невнимательности оператора возникали предпосылки к нарушению безопасности связи. Особенность М-228 заключалась в том, что она позволяла осуществлять передачу текста как в открытом, так и зашифрованном виде, для чего оператор должен был перед началом работы установить переключатель режима в соответствующее положение. За годы Второй мировой войны имели место по крайней мере два случая, когда по невнимательности операторов аппаратуры М-228, забывших перевести переключатель в необходимое положение, в эфир были переданы секретные сообщения в незашифрованном виде.  
Отдел С был вторым по численности среди подразделений Службы и отвечал за своевременную поставку в войска шифраппаратуры, кодовых книг и шифрдокументов, разработку правил и инструкций по безопасности связи войск. Важное место в деятельности отдела занимали организация радиоконтроля за соблюдением правил радиообмена в войсках, а также оценка практической криптостойкости шифров, используемых подразделениями связи армии США. Специалисты отдела разрабатывали специальные инструкции, исключающие возможность утери шифраппаратуры, а также тщательно анализировали все случаи, связанные с пропажей шифрдокументов и аппаратуры. Так, специалисты отдела были достаточно серьезно обеспокоены, когда к ним поступило сообщение о "захвате японскими войсками Сайджебы в Новой Гвинее". Как выяснилось, тревога была ложной - Сайджеба оказалась не шифрмашиной, а поселком в Новой Гвинее.   
Более серьезный случай произошел в феврале 1945 г., когда уже настоящая шифрмашина "Сайджеба" со всеми инструкциями, документами и комплектом роторов пропала во Франции, в районе города Колмар. Утеря произошла по вине военнослужащих 28 пехотной дивизии США. Под личным руководством верховного главнокомандующего экспедиционными силами союзников в Западной Европе генерала Д. Эйзенхауэра была проведена широкомасштабная поисковая операция с привлечением воздушной разведки, проверками на дорогах, в домах и т. д. Операция продолжалась более месяца и завершилась успешно - 12 марта 1945 г. шифрмашина была обнаружена и возвращена в дивизию.  
Основными "поставщиками" материалов радиоперехвата для криптоаналитиков Арлингтон-Холла являлись подразделения 2-го батальона радиоразведки, который был создан 2 апреля 1942 г. в результате увеличения численности и изменения структуры 2-й роты. При участии личного состава батальона в сентябре того же года была создан новый стационарный пост радиоперехвата в Винт-Хилл Фармс (штат Вирджиния), а чуть позднее - еще 2 поста, в штате Калифорния и на Аляске. В период Второй мировой войны численность батальона существенно возросла и одно время достигала приблизительно 5 тыс. человек.   
К середине Второй мировой войны подразделения батальона находились на территории США, Аляски, Алеутских и Гавайских островов, а также в Австралии, Индии и Африке. Посты радиоперехвата и радиопеленгования, находящиеся за пределами страны, входили в состав войск связи соответствующих армейских командований Отдельные подразделения батальона, например посты, расположенные в Беллморе (остров Лонг-Айленд) и Тарзане (штат Калифорния), использовались только для радиоконтроля за работой армейских радиостанций на территории США и к ведению радиоразведки не привлекались.  
Для решения возложенных на них задач подразделениями 2-го батальона использовалась различная аппаратура радиоразведки. На вооружении стационарных постов находились средне-, коротко- и ультракоротковолновые радиоприемные устройства SCR-243 и 244, SCR-607, 612 и др., а также средне- и коротковолновый радиопеленгаторы SCR-206 и 503.  
В состав подвижного поста, размещаемого на одной автомашине, входили радиостанция SCR-284 и комплекс радиоразведки SCR-558, состоящий из радиопеленгаторов SCR-206, 503 и радиоприемного устройства SCR-612.  
Подвижный пост на базе комплекса радиоразведки AN/VRD-1 размещался на двух автомашинах, каждая из которых была оборудована радиопеленгатором SCR-503, радиоприемными устройствами SCR-612, 613, радиомаяком RC-163, а также радиостанцией SCR-510.  
В связи с постоянной нехваткой личного состава в подчиненных ему отделах и подразделениях начальник Агентства безопасности связи полковник Кордерман обратился к руководству Женской вспомогательной службы армии WACS (Women's Army Corps Service) с просьбой выделить военнослужащих-женщин для прохождения службы в составе вспомогательных подразделений Арлингтон-Холл.   
Первая группа из 800 женщин прибыла в подчинение полковнику Кордерману в апреле 1943 г., а в последующем численность женского персонала в составе агентства безопасности связи возросла до 1500 человек. Высвобождавшиеся при этом военнослужащие-мужчины направлялись в подразделения батальона, дислоцированные за пределами США.

Последние реорганизации

Завершающий этап войны ознаменовался для Агентства безопасности связи новыми организационными переменами. В начале 1944 г. в результате проведенной реорганизации в нем были созданы четыре отдела: разведывательный, безопасности связи, вспомогательный, комплектования и подготовки личного состава. В декабре того же года Агентство было передано в оперативное подчинение Управлению военной разведки, при этом административное руководство Агентством осталось за Начальником войск связи.   
6 сентября 1945 г., через четыре дня после окончания Второй мировой войны руководством Военного министерства было принято новое решение, согласно которому Агентство безопасности связи было полностью выведено из подчинения Начальника войск связи и с 15 сентября преобразовывалось в Агентство безопасности Армии США.  
Пройдет еще 7 лет, и 24 октября 1952 г. президент Г. Трумэн поставит свою подпись в конце семистраничного меморандума, в соответствии с которым Агентство безопасности Армии наряду с аналогичными службами Военно-воздушных и Военно-морских сил войдет в состав вновь образованного, одного из наиболее засекреченных ведомств Пентагона - Агентства национальной безопасности США.

Литература

1. У. Диффи, М. Э. Хеллман. Защищенность и имитостойкость: введение в криптографию. ТИИЭР, 1979, том 67, № 3, с. 71-109.  
2. Б. Ю. Анин, А. И. Петрович. Радиошпионаж. М.: Международные отношения, 1996.  
3. Военный энциклопедический словарь. М.: Воениздат, 1984.  
4. G. R. Thompson, D. R. Dixie. The signal corps: The outcome (mid 1943 through 1945), Washinghton: US Army, Office of the Chief of military history, 1966.  
5. ULTRA and the Army Air Force in World War II. Office of Air Force History, US Air Force, Washinghton, D.C.,1987.  
6. D. Kahn. The Codebreakers. SPHERE Books LIMITED, London, 1973.  
7. J. Bamford. The Puzzle Palace. A Report on NSA, America's Most Secret Agency. Boston, 1982.