

Вадим Гребенников

# Радиоразведка Европы

Перехват  
информации



Вадим Гребенников

**Радиоразведка Европы.  
Перехват информации**

«Издательские решения»

## **Гребенников В.**

Радиоразведка Европы. Перехват информации /  
В. Гребенников — «Издательские решения»,

ISBN 978-5-44-935900-1

Любое государство сейчас не может существовать без технической разведки. Радиоразведка появилась вместе с радиосвязью в начале XX века. Книга рассказывает историю рождения и эволюции техники и методов радиоэлектронной разведки и контрразведки спецслужб Великобритании, Германии, Франции, Австрии и Швеции; описывает успехи радиоразведки этих стран по перехвату информации. «Кто владеет информацией, тот владеет миром». (Натан Ротшильд)

ISBN 978-5-44-935900-1

© Гребенников В.  
© Издательские решения

# Содержание

Предисловие	6
1. Рождение радиоразведки	11
2. Радиоразведка Австрии	15
3. Радиоразведка Швеции	23
Конец ознакомительного фрагмента.	28

# **Радиоразведка Европы Перехват информации**

**Вадим Гребенников**

*Редактор* Вадим Гребенников

*Дизайнер обложки* Вадим Гребенников

© Вадим Гребенников, 2019

© Вадим Гребенников, дизайн обложки, 2019

ISBN 978-5-4493-5900-1

Создано в интеллектуальной издательской системе Ridero

## Предисловие

Книга написана в продолжении развития темы «перехвата» информации и дешифровки переписки противника, которая была изложена в предыдущих книгах по истории криптологии, стеганографии и специальных (секретных) видов связи.

За свою историю разведка накопила большой опыт добывания информации, в том числе с использованием технических средств. Такие задачи инициируют исследования по созданию принципиально новых способов и средств разведки. С этой целью органы разведки ведущих стран имеют мощную научно-производственную базу.

В настоящее время разведку разделяют на агентурную и техническую. Хотя для практики это разделение условное. Условность состоит в том, что добывание информации агентурными методами (агентами) часто осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия – в преобладании человеческого или технического факторов.

Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента – разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее заказчику.

Применение технической разведки снижает риск задержания агента органами контрразведки или госбезопасности, за счет дистанционного контакта его с источником информации, а также создаёт возможность ведения разведки без нарушения госграницы средствами космической, компьютерной и радиоразведки иностранных государств.

Техническая разведка появилась в процессе технической революции XX века. В основу ее классификации по используемой технике положен физический принцип построения аппаратуры разведки. В соответствии с этим принципом техническая разведка делится на радиоэлектронную, компьютерную, оптическую, оптико-электронную, акустическую, гидроакустическую, химическую, радиационную, сейсмическую и магнитометрическую.

Нас будет интересовать радиоэлектронная разведка «SIGINT» (англ. Signals intelligence) (далее – РЭР), которая делится на радиотехническую, радиолокационную, радиотепловую, радиоразведку и разведку побочных электромагнитных излучений и наводок (далее – ПЭМИН).

1. Радиоразведка «COMINT» (англ. Communication Intelligence) – направлена на перехват радиogramм и сбор разведанных, основанный на приёме и анализе каналов радиосвязи противника. Радиоразведка посредством перехвата сообщений, исходящих от тех или иных командных инстанций, может получать информацию из самых надежных источников – штабов противника.

Сведения радиоразведки о радиостанциях противника, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления и т. п.

Этот вид разведки обладает следующими особенностями:

- действует без непосредственного контакта с объектами разведки,
- охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот,
- функционирует непрерывно в разное время года и суток и при любой погоде,
- обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации)
- добывает большое количество информации различного характера и содержания,

- получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени,
- малоуязвима и во многих случаях недостижима для противника,
- действует скрытно, поскольку противник, как правило, не в состоянии установить факт разведки.

2. Радиотехническая разведка «ELINT» (англ. Electronic intelligence) – вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (далее – РЛС), радионавигационных систем и систем связи, использует методы радиоприема, пеленгования и анализа радиосигнала. Средства радиотехнической разведки позволяют:

- установить несущую частоту передающих радиосредств;
- определить координаты источников излучения;
- измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);
- установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- определить структуру боковых лепестков излучения радиоволн;
- измерить поляризацию радиоволн;
- установить скорость сканирования антенн и метод обзора пространства РЛС;
- проанализировать и записать информацию.

3. Радиолокационная разведка – предназначена для получения радиолокационного изображения (обстановки). В радиолокаторе формируется зондирующий узкий, сканирующий по горизонтали и вертикали луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который, перемещаясь синхронно с зондирующим лучом, «рисует» на экране изображение объекта.

4. Радиотепловая разведка добывает информацию о признаках объектов, проявляющихся через их собственные электромагнитные излучения в радиодиапазоне.

5. Разведка ПЭМИН использует ту же радиоаппаратуру и методы, что и радиоразведка. Только эта аппаратура предназначена для улавливания очень слабых сигналов, то есть она более чувствительная.

Различают наземную, морскую, воздушную и космическую РЭР. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся:

- открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи,
- тактико-технические данные и особенности разведываемых активных радиоэлектронных средств и систем (далее – РЭС), составляющие их «электронный почерк»,
- типы РЭС: радиосвязи, радиолокации, радионавигации, различные телеметрические системы передачи данных,
- количество обнаруживаемых РЭС противника,
- местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Изучая технические характеристики и особенности РЭС противника, можно определить область их применения и принадлежность. Сопоставляя эти данные с уже известными, полученными разведкой по другим каналам, можно сделать вывод о назначении разведываемых технически средств.

Зная это и определяя типы и количество РЭС противника, можно установить дислокацию войсковых частей, военных баз, аэродромов и других объектов.

Для анализа и обработки добываемой информации очень важное значение имеют точная фиксация времени начала и конца работы излучающих РЭС и правильное определение их местоположения. Эти данные позволяют установить степень активности противника в определенной территориальной зоне.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемыми разведываемой страной впервые. Целью добывания технической информации является своевременная разработка аппаратуры и методов РЭР новых систем оружия и средств управления противника.

Для получения такой информации средствами РЭР ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками.

Особенности РЭР заключаются в следующем:

- действует без непосредственного контакта с объектами разведки;
- охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот;
- функционирует непрерывно в разное время года и суток и при любой погоде;
- обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации);
- добывает большое количество информации различного характера и содержания;
- получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени;
- малоуязвима и во многих случаях недостижима для противника;
- действует скрытно (противник, как правило, не в состоянии установить факт разведки).

Также нас будет интересовать и компьютерная разведка – целенаправленная деятельность по добыванию с помощью средств вычислительной техники (далее – СВТ) и программного обеспечения (далее – ПО) разведывательной информации, обрабатываемой в СВТ и информационно-вычислительных сетях (далее – ИВС), а так же информации об особенностях их построения и функционирования.

Целью компьютерной разведки является добывание сведений о предмете, конечных результатах, формах и способах деятельности субъектов, являющихся пользователями компьютерной сети и используемом аппаратном и программном обеспечении, протоколах управления и информационного взаимодействия и используемых средствах и методах защиты информации.

Важнейшая роль в достижении информационного господства отводится виртуальной разведке – разведке, ведущейся в информационных потоках, которые в гигантских количествах производятся всеми государственными и частными организациями, а также отдельными лицами. Компьютерную разведку ещё называют виртуальной разведкой.

Виртуальная разведка ведется в компьютерных сетях, средствах массовой информации (далее – СМИ) и непериодических изданиях, в том числе открытых и так называемых «серых», не имеющих грифа секретности, но не предназначенных для массового распространения.

Виртуальная разведка представляет собой целый комплекс взаимосвязанных действий оперативно-технического характера. Важнейшей технической компонентой виртуальной разведки является компьютерная разведка. Она делится на добывающую и обрабатывающую. Задача добывающей разведки состоит в получении данных, а обрабатывающей – в преобразовании данных в информацию и приведение ее в форму, удобную для пользователя.

Добывающая разведка бывает предварительной и непосредственной. Задача предварительной разведки – получение сведений о самой автоматизированной системе (далее – АС)

противника, обрабатывающей защищаемую информацию. Цель предварительной разведки – подобрать данные, необходимые для последующего проникновения в АС противника.

Цели предварительной разведки достигаются путем добывания открытых и закрытых сведений. К открытым сведениям можно отнести данные о характере и режиме работы АС объекта разведки, квалификации его персонала, составе и структуре самой АС, используемом ПО, протоколах управления и взаимодействия, средствах и методах защиты информации, используемых в АС.

Для получения этих сведений нет необходимости прибегать к приемам оперативной работы (подкупу персонала, краже документации и т. п.). Эти сведения, как правило, не являются закрытыми и могут быть получены при перехвате сетевого трафика интересующей АС или попытке установить сетевое соединение непосредственно с самой АС, когда по характеру получаемого отклика можно сделать соответствующие выводы.

Установление первичного контакта с АС противника, как правило, еще не дает доступа к интересующей информации. Для этого необходимо получить дополнительные сведения закрытого характера. К таким сведениям относятся пароли, коды доступа, информация о принятых в АС правилах разграничения доступа и сетевые адреса СВТ объекта.

Для получения подобных сведений существуют разнообразные шпионские программные средства. К ним относятся, например, программы перехвата всех команд, вводимых в АС. Другим средством являются программы считывания первых 128 бит каждого файла, в которых нередко помещается служебная информация о самом файле и об АС.

Существуют также специальные программы подбора паролей. Успеху подобных программ способствуют многочисленные ошибки в современном ПО, что объясняется его сложностью и относительной новизной. Помимо ключей, интерес представляет перехват кусков зашифрованного текста с заранее известным содержанием.

Это позволяет выделить из шифрограммы секретный ключ, который используется для дальнейшего криптоанализа всего текста. Сведения, собранные об АС противника подобным образом, открывают путь к добыванию информации, интересующей заказчика, т. е. к ведению непосредственной разведки.

На стадии непосредственной разведки, как и на всех остальных, добываются не только закрытые, но также «серые» и открытые сведения. Роль открытых сведений в достижении общей ситуационной осведомленности о противнике достаточно велика.

Важнейшим достоинством перехвата открытых сведений при ведении компьютерной разведки является то, что эти сведения могут быть получены без нарушения принятых в АС правил разграничения доступа к информации. Сбором и анализом открытых сведений в сетях официально занимается множество организаций, которые за определенную плату выполняют заказы на поиск той или иной информации.

Добывание закрытых сведений всегда связано с несанкционированным доступом (далее – НСД) к информации противника и имеет своим следствием утечку информации. Получение закрытых сведений осуществляется как в самой АС объекта, так и в ИВС, внешних по отношению к АС.

Во внешних сетях перехватываются те сообщения, которые объект разведки пересылает внешним адресатам, либо в случае виртуальной сети, те сообщения, которые циркулируют между отдельными сегментами АС. Программное проникновение в АС объекта с целью ведения разведки может осуществляться несколькими способами. Отдельную группу таких способов составляет проникновение через несетевые периферийные устройства (клавиатуру, дисководы и т. п.).

Наиболее многочисленная и динамично развивающаяся группа способов программного проникновения в АС противника – это проникновение из внешних сетей. Можно выделить два основных пути такого проникновения:

– проникновение с использованием паролей и идентификаторов, найденных в результате предварительной разведки;

– поиск уязвимостей и ошибок (к называемых «черных ходов») в аппаратном и программном обеспечении, используемом в АС.

При применении указанных способов проникновения, недостаточно лишь добраться до винчестера противника и «скачать» с него данные. Необходимо восстановить удаленные файлы противника и тщательно разобраться в полученном объеме сведений. Эту функцию выполняет обрабатывающая разведка.

Обработке подвергаются данные, полученные как в отдельном СВТ, так и в ИВС, при этом сеть представляет дополнительные возможности по обработке. Посредством анализа трафика можно контролировать гигантские потоки сведений, производить отбор, накопление и обработку не всех данных подряд, а только тех, которые представляют интерес для заказчика.

Для ведения экспресс-анализа в сети созданы специальные программы, так называемые «ноуботы» (англ. Knowbot – Knowledge Robot – робот знаний), которые способны перемещаться в ИВС от между СВТ и при этом размножаться, создавая копии. «Ноубот» вводится в компьютерную систему и, обнаружив интересующую его информацию, оставляет в этом месте свою копию, которая собирает информацию и в определенное время передает ее.

С целью исключения обнаружения в «ноуботе» могут быть предусмотрены функции самоперемещения и самоуничтожения. С помощью средств компьютерной разведки можно не только анализировать конкретные данные, циркулирующие во всей сети, безотносительно к их источнику, но и отслеживать деятельность конкретных организаций и отдельных лиц.

Особо следует подчеркнуть, что обработке подвергаются не только закрытые, но и открытые сведения. Соответствующий анализ открытых источников позволяет синтезировать информацию закрытого характера. По оценке специалистов изучение 10000 открытых документов позволяет при некоторых условиях получить 1 документ высшей степени секретности.

В связи с высокой степенью угрозы безопасности информации, обрабатываемой в ИВС, все большее количество пользователей сети применяют для защиты своей информации шифрование. По этой причине одной из задач обрабатывающей компьютерной разведки является применение криптоаналитического ПО.

Кроме вооруженных сил компьютерной и радиоразведкой занимаются государственные спецслужбы и правоохранительные органы, добывая при этом, в основном, оперативную информацию путем перехвата шпионских радиogramм и электронной переписки подозреваемых лиц. А теперь обо всем поподробней...

## 1. Рождение радиоразведки

С момента рождения радио в 1895 году и по мере его внедрения как средства связи и управления оно стало использоваться во всех странах в интересах государственной и военной разведки.

В 1902 году в Великобритании был опубликован рассказ Редьярда Киплинга под названием «Беспроволочный телеграф», в котором описывались опыты по перехвату радиосигналов. Процесс радиоперехвата в рассказе уподоблялся спиритическому сеансу – те же «обрывки посланий, долетающие невесть откуда, отдельные слова, а в целом – ничего не разберешь».

«Беспроволочный телеграф» был интересен тем, что в нем впервые открыто обсуждались вопросы, связанные с радиоразведкой. В рассказе было правильно показано, что в начале 1900-х годов для того, чтобы использовать эфир в качестве источника разведывательной информации, не требовалось ничего, кроме оборудования, которое позволяло слушать чужие радиопереговоры.

Однако по мере того, как такое оборудование получало все большее распространение, лица, общавшиеся между собой посредством радио, стали прибегать к помощи шифров, чтобы сделать содержание своих сообщений недоступным для других. Поэтому помимо перехвата эфирных сигналов для ведения радиоразведки вскоре понадобилось взламывать шифры, которые применялись для засекречивания передаваемых сообщений.

Уже в начале XX века ведущие мировые страны вели слежку за работой радиостанций своих противников и прослушивание их радиопередач. Известно, что с 1902 года британский флот, а с 1903 года американский флот в ходе учений опробовали перехват вражеских радиопереговоров.

Однако интенсивно разведка радиотехническими средствами стала использоваться воюющими странами и их союзниками с началом русско-японской войны в 1904 году. Так, британские корабли систематически перехватывали радиопередачи русских боевых кораблей, находившихся в Средиземном море (в том числе осуществлявших переход на Дальний Восток).

В 1914 году в Европе началась Первая Мировая война. 1 августа Германия объявила войну России, а 3 августа – Франции, а также нейтральной Бельгии, отказавшейся пропустить немецкие войска через свою территорию. 4 августа Великобритания со своими доминионами объявила войну Германии, а 6 августа Австро-Венгрия – России.

В августе 1914 года войну Германии объявила Япония, в октябре – на стороне блока Германии и Австро-Венгрии в войну вступила Турция, а в октябре 1915 года – Болгария. Италия, изначально занимавшая позицию нейтралитета, в мае 1915 года под дипломатическим давлением Великобритании объявила войну Австро-Венгрии, а 28 августа 1916 года – Германии.

С первых месяцев войны перехват радиосообщений противника позволил получать ценные сведения о его намерениях, о расположении и перегруппировке неприятельских войск. Этому способствовало нарушение элементарных правил радиообмена со стороны штабов армий и фронтов, передававших по радио секретные приказы и распоряжения открыто или с применением несложных шифров.

Воюющие стороны, убедившиеся в утечке информации через радиосвязь, вскоре стали применять более сложные шифры и строже регламентировать свои радиопередачи. Однако нарушения радиодисциплины продолжались.

Наблюдая и изучая характерные особенности действующих радиосвязей противника, их интенсивность, позывные, стабильность, рабочие частоты, тон сигнала работающих радиостанций, «почерк» радистов, продолжительность и время передач старых и вновь появившихся радиостанций, незначительные признаки нарушения радиообмена и т. п., радиоразведка была

в состоянии вскрывать оперативные замыслы командования, следить за перемещением войск и получать другие важные сведения о противнике.

Если в начале войны для радиоразведки использовались приемные устройства связных радиостанций, то в последующие годы воюющие стороны стали применять специальные радиоприемники и создавать первые подразделения службы радиоразведки.

Радиопеленгаторы как средство войсковой и морской радиоразведки впервые появились в действующих армиях Российской империи, Великобритании, Германии, Австро-Венгрии в 1915—16 годах.

Радиопеленгаторная аппаратура внесла новое содержание в радиоразведку и принципиально расширила ее возможности. С помощью радиопеленгаторов стали определять местонахождение вражеских радиостанций и тем самым устанавливать районы нахождения штабов, частей и соединений, время начала и направление их перемещения.

Британская радиоразведка, имея хорошо организованную службу радиоперехвата и криптоанализа, систематически дешифровывала немецкие секретные радиограммы, передаваемые не только штабами частей и соединений армии, но и правительством, генеральным штабом, посольствами и другими ведомствами.

Особенно успешно действовала военно-морская разведка Великобритании. Ее центром была «комната 40» британского адмиралтейства, где высококвалифицированные криптоаналитики расшифровывали перехваченные радиограммы.

Британская радиоразведка сыграла важную роль в морской войне своего флота с немецкими подводными лодками (далее – ПЛ), блокирующими Великобританию со всех сторон. Криптограммы, посылаемые германским морским командованием по радио своим ПЛ, перехватывались британцами и дешифровывались.

Они достали с морского дна несколько кодовых книг Военно-морского флота (далее – ВМФ) Германии, находящихся в затопленной немецкой ПЛ, и пользовались ими при дешифровке радиограмм.

В истории британской радиоразведки важное место занимает Ютландское сражение. В конце мая 1916 года британцы перехватили переданный немцами по радио секретный приказ о выходе немецкого ВМФ в море для нанесения внезапного удара по британскому ВМФ. Британцы дешифровали содержание приказа и стали скрытно готовиться к отражению атаки.

В результате британцы навязали немцам неожиданное для них сражение в 90 милях к западу от северной оконечности Ютландского полуострова, в котором немцы понесли тяжелые потери.

Важный след оставила британская радиоразведка и в нашумевшем в свое время заявлении Президента США Вудро Вильсона, сделанном 1 марта 1917 года, накануне вступления США в Первую Мировую войну на стороне союзников.

В нем было заявлено, что министр иностранных дел Германии Артур Циммерман предложил мексиканскому правительству присоединиться к Германии, чтобы объявить США войну.

Естественно возник вопрос, каким образом немецкий совершенно секретный документ попал на стол американского президента. Оказалось, что британская радиоразведка перехватила шифртелеграмму Циммермана, переданную по радио, дешифровала ее и немедленно передала американскому послу в Лондоне.

Немецкая радиоразведка в Первой Мировой войне также выдавала весьма ценные сведения о противнике военному командованию. Известно, что в отдельные периоды войны немцы дешифровывали в сутки до 300 секретных радиограмм своих противников.

Начальник разведывательного управления Верховного командования Вооруженных сил Германии в период 1913—19 годов Вальтер Николаи в своих мемуарах поведал, что достоверным источником сведений являлись перехваченные русские радиопередачи.

В связи с этим коротко расскажу о событиях, которые произошли в Восточной Пруссии в августе 1914 года. Штаб второй русской армии генерала Александра Самсонова, не имея связи со своими наступающими корпусами, передал им по радио открытым текстом ряд секретных приказов, которые были перехвачены немецкой радиоразведкой.

В результате немцы получили ясную картину действий противника на ближайшие дни. Немецкое командование грамотно использовало полученные разведанные, и после активных действий немцев русская армия была разгромлена.

Австрийская радиоразведка действовала весьма успешно с самого начала Первой Мировой войны и информировала свое верховное командование и германское командование о всех перехваченных приказах и донесениях, которые передавались по радиотелеграфу.

Книга начальника разведывательного бюро Генерального штаба (далее – ГШ) Австрии генерала Макса Ронге содержит большой фактический материал о деятельности австро-венгерской радиоразведки за весь период Первой Мировой войны.

Она содержит многочисленные примеры работы радиоразведки, данные которой позволяли оценить оперативную обстановку до начала проведения той или иной операции и послужили основанием для планирования и проведения боевых действий.

Так, например, во время Галицийской операции, в начале сентября 1914 года, когда между 1-й и 2-й австрийскими армиями образовался разрыв, австрийская радиоразведка получила сведения о том, что в направлении прорыва двигаются крупные соединения русских. В результате австрийское командование приняло решение об отходе всех австрийских армий за реку Сан.

**Болгария** первый опыт ведения радиоразведки в армии и на флоте получила в ходе Балканской войны 1912—13 годов. На флоте в этих целях накануне и в ходе Первой мировой войны использовались стационарная радиостанция «Франга» (около н. п. Голяма Франга, ныне – Каменар), корабельная радиостанция на борту крейсера «Надежда», четыре береговые радиостанции (2 стационарные в н. п. Галата и Карантината, 2 подвижные).

Болгарский офицер Г. Д. Сколуфанов вспоминает, что для того, чтобы избежать помех от радиостанций вооруженных сил Болгарии турки прибегали к хитрости. Они начинали радиопередачу на волне 600 м, а когда понимали наше вмешательство, переходили на волну 1200 м. Факт того, что турецкие радиотелеграфисты меняли частоты радиосвязи, защищая свою информацию, показывает, что они опасались перехвата своих радиограмм.

**Италия** до Первой мировой войны проявляла к радиоразведке и криптоанализу незначительный интерес. Тем не менее, к началу войны там появилось несколько весьма одаренных радиоразведчиков. Лучшим среди них был Луиджи Сакко, 32-летний лейтенант инженерных войск, служивший на радиостанции Верховного командования. Первых результатов в радиоразведывательной деятельности он добился в ходе итало-турецкого конфликта 1911 года.

Сакко, который возглавлял итальянскую службу перехвата, удалось самостоятельно дешифровать перехваченные радиограммы. Восстановленные им участки открытого текста оказались настолько ценными, что его назначили главой дешифровального отдела при Верховном командовании. Отдел в целях конспирации назывался Шифровальным подразделением и первоначально состоял всего из 3-х человек. Однако к концу войны в нем служили уже несколько десятков сотрудников.

Итальянские радиоразведчики и криптоаналитики добились полного чтения австро-венгерских криптограмм во время битвы при Гориции в августе 1917 года. Растущий опыт итальянских разведчиков помогал им решать все более сложные задачи, например, вскрыть австрийский дипломатический код.

Готовой к войне в эфире оказалась и радиоразведка Франции. Заслуга в этом принадлежала созданным еще в довоенное время дешифровальным органам, более мощным и лучше организованным, чем в других странах. Криптбюро, созданное Ф. Картье в военном мини-

стерстве, было обеспечено мобилизованным персоналом. В первые дни интенсивность радиосвязи противника была низкая, но когда немецкие войска в начале августа 1914 года пересекли границу Франции, выйдя за пределы своих телеграфных линий, количество их радиопередач резко увеличилось.

Сначала французские станции радиоперехвата находились лишь в крупных крепостях и в 3-х специальных пунктах перехвата, а 6 радиопеленгаторных станций находились вдоль линии фронта. Позднее к ним добавились еще 2 пункта перехвата в Париже – один на Эйфелевой башне, другой – на станции парижского метро «Трокадеро».

Радиоразведчикам военного министерства приходилось оказывать помощь МИД в чтении дипломатической переписки на линии связи Берлин – Мадрид. Подопечные Картье читали также и военно-морскую шифрпереписку немцев, поскольку французский флот не имел в своем штате криптоаналитиков.

В частности, ими был вскрыт шифр немецких ПЛ. Французы обнаружили, что каждую полночь подпольная радиостанция в г. Науне посылала немецким ПЛ в Средиземном море время выхода и маршруты французских судов, отплывавших из Марселя. Радиоразведчики перехватывали сообщения немецких шпионов, а криптоаналитикам требовалось не более часа, чтобы их дешифровать. В результате вносились изменения в расписание рейсов и маршруты перехода судов. Многие из раскрытых кодов Германии французы отправляли англичанам.

Уже к 1915 году Криптбюро превратилось в первое в мире полноценное государственное ведомство радиоразведки. Оно имело в штате несколько десятков человек, из которых 9 были криптоаналитики. Главе Криптбюро подчинялась также шифровальная служба ГШ. По мнению Ф. Картье его подчиненные перехватили за время Первой мировой войны более 100 миллионов слов.

Радиоразведку русского флота в водах Балтийского моря, перехват и дешифрование дипломатической переписки Германии в ходе Первой мировой войны, несмотря на проводимую политику нейтралитета, осуществляли и подразделения радиоразведки Швеции.

Все это свидетельствует, что радиоразведка во время Первой Мировой войны развивалась и как постоянно действующая структура, как и один из основных видов разведки вооруженных сил Российской империи, Австро-Венгрии, Великобритании, Германии, Италии, США, Франции, Болгарии, Швеции и Японии.

Процессы строительства радиоразведки как структуры и совершенствования ее деятельности как вида разведки протекали в этих государствах со своими особенностями и различными результатами. Тем не менее, общими чертами этого периода являлись специализация сил и средств радиоразведки, консолидация усилий различных ведомств в области добывания информации и криптоанализа, организация взаимодействия с союзниками.

## 2. Радиоразведка Австрии

Должность начальника разведгруппы Разведывательного Бюро ГШ «Эвиденцбюро» Вооруженных сил Австро-Венгрии перед Первой Мировой войной занимал Максимилиан Ронге. Он в 1911—12 годах добился включения в состав группы нескольких офицеров, специалистов в области шифрования и дешифрования.

Он в своей книге «Разведка и контрразведка», изданной в 1939 году, привел интересные сведения о работе австрийской радиоразведки на фронтах Первой Мировой войны. Официально австрийская служба радиоразведки и дешифровки появилась в структуре Разведывательного Бюро только к апрелю 1917 года. В дальнейшем появились дешифровальные службы и группы на фронтах.

Особенно выдающимся специалистом в сфере дешифровки был капитан Герман Покорный, начальник русского отделения дешифровальной службы. Соответственно, можно констатировать, что австрийское командование вступило в войну с высококвалифицированными кадрами специалистов-радиоразведчиков, что в дальнейшем принесло свои плоды.

Уже в начале войны при австрийских армейских командованиях находились рации, передававшие перехваченные депеши в разведывательный отдел (фронтальной центр дешифрования). Эти рации занимались исключительно наблюдением за рациями соединений русской армии.

Очень ценным источником информации оказалась русская радиотелеграфная переписка. Русские пользовались своим радиотелеграфом так легкомысленно, как будто не предполагали о наличии радиоприемников, которые можно настроить на соответствующую волну.

К тому же поначалу русские радисты нередко вставляли открытый текст в зашифрованный. Вскоре одновременное использование открытых и зашифрованных текстов в сообщениях было запрещено, но было уже слишком поздно, и оно сыграло свою негативную роль.

10 сентября 1914 года во время сражения под Львовом создалось критическое положение. Русским не удалось разбить наше северное крыло; южное же крыло, во главе с начальником генштаба фон Конрадом, двигалось к Львову. Радиоразведка получила секретные сведения о том, что русские войска движутся по направлению к пустому пространству, образовавшемуся возле 1-й армии. Так как резервов для обеспечения тыла фронта у австрийцев не было, то было принято решение об отступлении.

14 сентября австрийцы перехватили распоряжение Ставки русских войск о необходимости полностью зашифровывать все военные сообщения, передаваемые по радио. Однако переход на зашифрованные радиопередачи не изменил положения дел. Имея большой опыт по перехвату русского радиообмена, на основании его анализа австрийцам удалось дешифровать русский шифр. Дешифровка первой русской радиограммы заняла около 4-х суток, после чего австрийцы продолжали вести эффективную радиоразведку.

При отступлении австрийских войск в Галиции со взятием русскими войсками Перемышля австрийская радиоразведка перехватила радиограмму, посланную командиром русского кавалерийского корпуса генералом Александром Новиковым, которая представляла большую разведывательную ценность. Эта радиограмма была быстро дешифрована и представлена немецкому командованию.

Примерно в это же время русские впервые сменили шифр. Сами строки остались без изменений, но изменился порядок выбора строк для зашифрования. Новый шифр был вскрыт Покорным 19 сентября в течение нескольких минут: все трудности отпали, когда одна из русских радиостанций передала зашифрованную новым шифром телеграмму, переданную еще до смены шифра.

Она не имела нового шифра и сообщила об этом по радио передающей станции, с которой последовала повторная передача этой же телеграммы, но зашифрованной старым шифром, что позволило дешифровальщикам легко вскрыть новый шифр.

Кроме того, новая шифрсистема не представляла серьезных трудностей для криптоаналитиков, поскольку в шифртексте сохранялась структура часто используемых в открытом тексте слов, таких как «атака», «дивизия», которые полностью шифровались одной строкой таблицы.

Первую важную шифртелеграмму Покорный прочитал 25 сентября. Это было длинное донесение Новикова о результатах разведки с примечанием в конце: «Я принял решение не форсировать Вислу». Шифртелеграмма была отправлена в 08—40 утра, а в 16—00 офицер связи довел до сведения немецкого штаба ее содержание. Знание принятого Новиковым решения обеспечило успех действий австро-германских войск в начальной стадии битвы на реке Висла.

Другой пример: из телеграммы полковника русской кавалерийской дивизии князя Ингаллица немцы узнали о готовившемся наступлении на крепость Перемышль. Предупрежденный об этом комендант крепости успешно отражал атаки, пока наступление австрийских войск не вынудило нападавших в середине октября снять осаду крепости. Во время этого наступления группа Покорного читала ежедневно до 30 русских шифртелеграмм.

4 октября 1914 года австрийская радиоразведка перехватила радиogramму русского полковника князя Енгальчева из 10-й кавалерийской дивизии в Санок. Из нее стало известно о предполагавшейся атаке на юго-восточных фортов Перемышля, о чем было немедленно оповещено по радио командование крепости. Капитан Покорный продолжал неустанно работать над дешифровкой радиоперехвата, и ему удавалось прочитать до 30 телеграмм в день.

11 октября немецкая армия под командованием Августа фон Макензена вклинилась в русскую оборону. В 14—10 следующего дня начальник штаба одной из русских армий, по которым был нанесен удар, передал по радио длинную шифровку. Кроме даты запланированной атаки в шифровке указывалась наиболее уязвимая зона в боевом порядке этой армии — стык между ее войсками и армией соседа.

На следующий день дешифрованная и переведенная радиogramма уже лежала в штабе немецких войск Восточного фронта, а ее содержание было немедленно передано Макензену. В 19—30, имея перед собой карту со схемой расположения русских, он отдал приказ о переходе подчиненных ему войск в наступление по всему фронту с нанесением главного удара в стык двух армий.

К этому времени русские ежедневно меняли порядок использования шифрalfавитов, но по-прежнему оставляли без изменений сами шифрalfавиты. В результате австрийские дешифровщики без перебоев читали их шифрпереписку. Поток информации, добываемой с помощью радиоперехвата, не сокращался. Немцы уже настолько привыкли к этому, что 19 октября Макензен не отдавал приказов до тех пор, пока не были получены сведения от дешифровщиков.

Следующий день стал черным для дешифровальной группы. В перехваченной шифртелеграмме 4-й русской армии содержалось предупреждение о том, что немцы имеют ключи к русскому шифру. Русские сумели захватить ключи к немецкому шифру и предположили, что аналогично мог поступить и противник. В действие был введен новый шифр, причем на этот раз — с заменой всех элементов шифрсистемы.

На Восточный фронт опустился занавес молчания. Лишенные глаз и ушей, армия Макензена к 21 октября оказалась в «мешке». Русские предвкушали победу и уже заказали поезда для вывоза военнопленных. Но на следующий же день группа Покорного вскрыла новый шифр, и в немецкий штаб вновь пошел поток ценной информации. Из него немцам стало известно

слабое место в кольце русских войск. К 25 октября 1914 года кольцо окружения было успешно прорвано.

Ежедневно австрийская служба радиоперехвата наблюдала за передвижением русских войск. 7 ноября она успела предупредить немецкую армию о готовившейся на нее атаке, благодаря чему серьезно подготовленное нападение успеха не имело. 3-й кавказский корпус 4-й русской армии и два соседних корпуса столкнулись друг с другом, и при этом возникло замешательство.

Оба командующих армиями яростно «бомбили» друг друга телеграммами, что доставило австрийцам большое удовольствие. Не меньшую радость доставил им приказ командования 5-й русской армии, требовавший от генерала Орановского посылать все указания по радио, так как восстановление разрушенных линий связи на театре военных действий требовало слишком много времени и сил. Этот приказ давал нам возможность беспрепятственно отслеживать большую часть мероприятий на Восточном фронте.

Служба радиоперехвата представляла бесценную информацию австро-германскому военному командованию. Можно было определить намерения русского командования и обеспечить учет вооруженных сил противника. В результате уже к концу октября была установлена точная дислокация частей, до дивизий включительно.

13 ноября был перехвачен и дешифрован приказ о переходе на следующий день во всеобщее наступление русской армии вглубь Германии, после чего сразу попал на стол канцелярии Главнокомандующего Восточным фронтом. Из этого приказа было, видно, что русские не имели никакого представления об угрозе их северному флангу и о силах перешедшей 12 ноября в наступление 9-й германской армии, которая расценивалась ими в один корпус.

20 ноября какой-то офицер связи 4-й русской армии передал по радио другому офицеру, что действующий шифр известен противнику. Затем австрийцы узнали из другой радиogramмы, что русские раскрыли немецкий шифр и поэтому узнали о том, что их шифр тоже известен противнику.

В результате русские заменили шифр, после чего австрийские и немецкие посты радиоперехвата скупуплезно собирали новые шифровки. К 22 ноября общими усилиями удалось раскрыть и этот новый шифр. Криптоаналитикам помогло, что русские, привыкшие к шаблону, придерживались привычной им шифровальной системы.

К сожалению, первым переданным сообщением было известие о прорыве немецкого окружения под Лодзью. Русские сообщения позволяли точно следить за действиями немецких частей.

В начале декабря австрийцы перехватили следующую русскую радиogramму: «Шифровальный ключ, не исключая посланного в ноябре, известен противнику». Тем не менее, русские продолжали пользоваться старым шифром. То ли у них было недостаточно других средств связи, то ли не было в запасе нового шифра, или же они считали достаточной частую смену позывных радиостанций, что во всяком случае удлиняло дешифровальную работу.

6 декабря 1914 года генерал Новиков сообщил, что он неожиданно получил приказ прикрывать отход 19-го русского корпуса. Это было первым признаком того, что русская армия начала свое отступление, по крайней мере, на северном фланге.

14 декабря новый русский шифр лишил нас источника сведений. Раскрытие нового шифра было сложным делом. Однако совместная кропотливая работа майора Глумака, капитана Покорного и обер-лейтенантов Земанека и Маркететти дала возможность его раскрытия в течение нескольких дней.

К весне 1915 года в русских войсках полностью отказались от старой системы шифров и стали применять простой шифр Цезаря. Большое количество таблиц, использовавшихся в условиях ведения активных боевых действий, и ежедневная смена ключей ставили непо-

сильную задачу перед связистами. В этих условиях вскрытие очередного русского шифра для дешифровальной службы не составило почти никакого труда.

Чтение русских криптограмм позволило принимать время от времени такие меры, которые были единственно правильным тактическим решением в данной ситуации. Российский ГШ был озадачен прозорливостью противника. Однажды немцы оставили занимаемые ими позиции за 2 дня до начала большого наступления русских войск. Одним из объяснений точного соответствия решений немецкого командования создавшейся обстановке русские считали использование им аэрофотосъемки и агентурной разведки.

Но постепенно крепло убеждение, что противник читает русскую шифрпереписку. Когда немецкое весеннее наступление 1915 года достигло апогея, русские опять сменили шифр. Но эта смена доставила больше хлопот им самим, так как почти все шифровки, переданные по радио в первые 2 дня после смены шифров из-за допущенных ошибок так и не были прочитаны адресатами.

В марте 1916 года австрийская радиоразведка получила стройную организацию, при этом для каждой станции радиоперехвата был определен определенный участок Восточного фронта. Во время русского наступления австрийцы оказали большую помощь немецким войскам, перехватив соответствующие приказы русского командования.

Главным руководителем австрийской радиоразведки был назначен капитан Болдескул, занявший место майора Покорного. Болдескул получил в подчинение 6 станций или групп радиоперехвата, которые находились в Барановичах, Ковеле, Берестечке, Бродах, Бржезанах и Коломые.

Австрийцы ежедневно дешифровывали до 70 радиogramм с оперативными приказами, сводками, о перемещениях командиров и т. п. Новые правила радиопередачи и новый шифр, объявленные 16 июня, вызывали недовольство русских штабов вследствие их сложности.

Ввиду этого ряд штабов продолжал пользоваться старым шифром и правилами, что в огромной степени облегчало раскрытие нового шифра. Штаб гвардейской группы, включенной в состав 8-й армии, передал в незашифрованном виде ключ нового шифра.

За этим последовал взрыв возмущения в штабе 8-й русской армии и введение штабом Юго-Западного фронта нового шифра. При этом было передано сообщение с помощью старого шифра, что при подготовке криптограммы вторичной перешифровки не требуется.

23 мая 1915 года Италия объявила войну Австро-Венгрии, поэтому австрийская радиоразведка работала и на итальянском фронте. Сначала она встречала затруднения из-за неспособности дешифровывать перехваченные радиogramмы. Однако со временем австрийцы хорошо изучили принципы шифрования итальянских радиogramм и стали их читать.

После того, как итальянская полевая радиослужба начала передавать не только сведения, касающиеся непосредственно службы связи, но и оперативные распоряжения, австрийцы ежедневно стали дешифрировать до 50, а в отдельные сутки до 70 криптограмм.

Тем не менее, итальянцы уже в начале 1916 года располагали большим количеством станций радиоперехвата. Так, в течение одного полугодия они смогли подслушать около 5200 радиоразговоров, что причинило австрийцам большой вред.

К этой работе ими было привлечено большое количество дезертиров и перебежчиков, знавших немецкий язык. В октябре 1916 года к ним перебежал начальник одной станции радиоперехвата, детально их ознакомивший с нашей организацией прослушки.

Прослушка, прежде всего, давала данные тактического порядка, а, кроме того, давала высшему командованию ценные сведения и обеспечивала проверку данных других видов разведки. Это было важно, поскольку противник умышленно направлял к нам перебежчиков для дезинформации. Они нередко обладали такой ловкостью и смелостью, что им удавалось вернуться обратно к своим.

Свыше 30 австрийских радиостанций осуществляли непрерывное наблюдение за таким же количеством итальянских станций. Каждая перехваченная радиограмма дешифровалась австрийцами в кратчайший срок.

22 февраля итальянцы ввели новую весьма остроумную систему позывных для радиостанций. Над ней австрийцам пришлось долго ломать голову, но все же к 7 марта она была раскрыта и сообщена персоналу радиостанций. 30 марта 1916 года итальянское главное командование запретило дальнейшее применение шифра «Cifrario rosso» в радиообмене в связи с подтвердившимся подозрениями о частичной компрометации этого шифра. На самом же деле он был раскрыт целиком и полностью.

Известный интерес для австрийцев представляла радиосвязь между итальянской главной квартирой в Удине и отдельным корпусом в Валлоне, хотя ею сравнительно мало пользовались благодаря исправности подводного кабеля между Корфу и Италией. Тем не менее, преодолев первоначальные затруднения, наши мощные радиостанции в Сараево, Петервардейне, Мостаре, Каттаро и Скутари добыли ряд важных сведений, передача которых продолжалась с помощью шифра «Cifrario rosso».

Кроме того, радиостанции в Скутари было передано все, относившееся к шифрам итальянского флота. В кратчайший срок она использовала эти материалы и оказала поддержку морской станции из Пола. В самой Албании итальянцы пользовались шифром «Менгарини», ключ которого был куплен австрийской разведкой еще до войны. Это сослужило хорошую службу радиостанции в Скутари и немецкому дешифровальному отделу в Ускубе.

Болгария вступила в Первую мировую войну 14 октября 1915 года на стороне Германии и Австро-Венгрии, объявив войну Сербии. 27 августа 1916 года Румыния объявила войну Австро-Венгрии, поэтому австрийская радиоразведка работала и на румынском фронте.

Вначале дешифровка румынских радиограмм была сопряжена с большими трудностями, но вскоре эта работа полностью себя оправдала, поскольку румыны, как и русские, передавали по радио оперативные приказы. Благодаря этому, австрийцы получили полную картину обстановки на фронте.

Так, австрийской радиоразведкой был перехвачен детальный оперативный приказ о контрнаступлении 14 сентября 1916 года добруджской армии, усиленной войсками из Трансильвании. Уже 16 сентября разведывательное бюро смогло передать в штаб 1-й армии в Колошвар (Клаузенбург) первые дешифрованные радиограммы, относившиеся к румынским войскам в Трансильвании.

Для радиоразведки наступили лучшие времена. В Софии был организован радиоразведывательный центр во главе с капитаном Янши, помощником которого был назначен капитан Маросан, имевший уже большие заслуги в деле дешифровки.

В этот центр поступали перехваченные сообщения не только от болгарских радиостанций перехвата, но и с радиостанций на румынском фронте. После дешифровки они передавались главному командованию и в армейскую группу Макензена, объединившую 1-ю и 9-ю армии.

Хоть румыны строго и запрещали незашифрованную радиопередачу, но с зашифрованными радиограммами обращались настолько неосторожно, что австрийцам пришлось выделить дополнительного дешифровальщика штабу 1-й армии для разгрузки радиостанции перехвата в Софии.

В начале войны с Румынией русские прилагали все усилия к тому, чтобы своим наступлением содействовать ожидавшемуся успеху. Благодаря радиоперехвату группы капитана Болдескула, получившей затем название «Австро-Норд» (группа капитана Янши стала называться «Австро-Зюйд»), наступательные намерения русских всегда своевременно выявлялись.

24 сентября для дешифровальщиков стало «черным» днем. Из-за потери 6-м русским кавалерийским корпусом шифров военного министерства для радиосвязи, радиограмма добруджской армии запрещала передачу оперативных приказов по радио.

Одновременно румынские сухопутные радиостанции прекратили передачу. Продолжала действовать лишь радиосвязь между морским ведомством и дунайской флотилией и связь главной квартиры с добруджской армией. 6 ноября радиогруппа дунайской русской армии перестала пользоваться «шифром службы связи №14» из-за его вероятной компрометации.

17 декабря радиопередача на русском юго-западном и на русско-румынском фронтах снова полностью прекратилась, поскольку радиостанция 1-й терской казачьей дивизии была захвачена противником. Радиосвязь стала «оживать» лишь с 21 декабря, причем стал применяться шифр, введенный 14 декабря.

Очевидно, русские шифровальщики не хотели «головной боли». В то же время австрийцам попались французские зашифрованные радиограммы, появившиеся в связи с прибытием для реорганизации румынской армии французской военной миссии во главе с генералом Анри Бертелло.

В 1917 году в радиоразведке была создана организация «Австро-Вест». Радиопеленгаторные станции, существовавшие до сих пор лишь в виде опыта, получили определенную организацию и должны были путем ежедневных измерений проверять дислокацию итальянских радиостанций.

На юго-западном фронте наряду с немногими отдельными станциями, были созданы следующие группы по 4 станции в каждой:

– «Пенкала Боцен» – в составе 4-х таких групп (Финоккио, Обербоцен, Тоблах, Крейцберг;

– «Пенкала Виллах» – в составе 8 отдельных станций;

– «Пенкала Адельсберг» – из 2-х групп (Адельсберг, Буйе).

Генерал Бороевич приказал особо хорошо обеспечить «Пенкала», поскольку итальянцы имели на фронте Изонцо большое число радиостанций – не менее 80, из них около 30 мощных. Каждой группе или отдельной станции была отведена определенная зона прослушки с таким расчетом, чтобы за каждой радиостанцией противника наблюдали 2—3 станции.

Дешифровку радиограмм осуществляла «Пенкала» юго-западного фронта, только в случае смены позывных или шифра криптограммы отправлялись в Баден. Радиостанции в Албании принимали помимо итальянских и сербских радиограмм, зашифрованных самыми простыми шифрами, еще французские. Из 3-х французских шифров немцы раскрыли 2, австрийцы – 1.

24 октября 1917 года в разгар наступления австро-германских войск на итальянском театре военных действий для «Пенкала» выдался удачный день. Одна за другой итальянские радиостанции подавали очень приятный сигнал: «свертываемся».

На некоторое время «Пенкала» были обречены на бездействие, поскольку шифр «Cifrario rosso» был заменен новым шифром ГШ, раскрытие которого потребовало кропотливой работы. Тем временем, 21 ноября были перехвачены радиограммы, указавшие на прибытие 46-й французской пехотной дивизии.

В ночь на 23 ноября 1917 года по приказу начальника итальянской радиосвязи все радиостанции сообщили центральной станции о своем местонахождении и расположении отдельно стоящих штабов. Благодаря этому, австрийцы быстро установили дислокацию всех итальянских соединений, включая и находившиеся поблизости в резерве.

Группам «Пенкала» пришлось заняться раскрытием нового шифра итальянских стационарных радиостанций, которые были включены в полевую сеть связи. Кроме того, итальянский офицер связи при салоникской армии стал пользоваться новым шифром.

Тем же шифром начальник итальянской военной миссии в Румынии генерал Ромен телеграфировал своему главному командованию о положении румынских и русских войск. Делал он это как раз в тот момент, когда русские радиостанции замолчали, за что австрийцы были ему очень признательны.

«Пенкала Баден», кроме того, должна была обрабатывать радиоперепику Италии со своими колониями, которая стала осенью весьма оживленной. Из нее стало известно о прекращении призыва в войска населения Северной Африки и других колоний. Это было особенно важно, поскольку после полученных потерь у итальянцев осталось мало сил для сопротивления.

Прибытие англичан и французов в Италию поставило перед австрийскими мастерами радиоразведки и дешифровки совершенно новые задачи. Трудности были связаны с тем, что первоначально войска находились на отдыхе, поэтому радиопередач было мало. Тем не менее, австрийцами еще на Балканах был накоплен большой материал по французскому радиотелеграфу. Первая французская радиограмма была перехвачена 23 декабря 1917 года.

Осознание важности и успешности работы австрийской радиоразведки содержал доклад итальянской следственной комиссии о сражении при Карфрейте:

«Достаточно указать на высокий уровень развития у противника радио подслушивания, дополненный изумительными достижениями по дешифровке шифров. Благодаря этому, противник выяснил наши пути отхода, определяя наши радиостанции и расшифровывая их радиограммы. Документы, захваченные после окончания войны, показывают, что противником были раскрыты почти все наши шифры, включая наиболее сложные и самые секретные».

Характерно, что как только итальянцы получили от дезертира немецкий радиоприемник, они тотчас же завели такие радиоприемники у себя. Показательно также, что ни один из австро-германских штабов не хотел отказаться от своих «Пенкала», когда нужно было уменьшить их число при сокращении фронта.

В результате принятого главным командованием решения маршал Конрад получил «Пенкала Боцен», генерал Борович – «Пенкала Сен-Вито», а эрцгерцог Евгений – «Пенкала Удине». Число радиогрупп было сокращено до 6, поэтому кроме указанных «Пенкала» остались только группы Финоккио и Штадлен.

Нараставшая в результате революций 1917 года дезорганизация русской армии оказала отрицательное воздействие и на ее службу радиосвязи. Пропорционально снижению дисциплины в войсках росла болтливость радистов. В начале года только в течение одного дня австрийская дешифровальная служба прочла более 300 русских шифртелеграмм, из чего следовало, что служба обеспечения безопасности связи в России быстро разваливалась.

С начала 1918 года станции телефонной прослушки, освободившиеся на русском фронте, позволили увеличить их число на юго-западном фронте до 82. Это было особенно важно в связи с тем, что условия местности и редкие боевые столкновения сильно уменьшили количество пленных и перебежчиков.

Вместе с тем налаженная итальянцами проводная связь ослабила эффективность работы австрийской радиоразведки. Однако благодаря офицеру связи при итальянском 20-м корпусе, который начал в марте по несколько раз в день передавать зашифрованные радиограммы, австрийцы оказались в курсе всех боевых действий.

Были результаты и у «слухача» на Кастеллачио – лейтенанта Кареты, и у «слухачей» на Пазубио – лейтенантов Торзиелло и Адамо. В апреле австро-германские войска совершенно прекратили пользование радиосвязью, так как была замечена активность итальянцев в деле радиоперехвата. Поэтому по радио разрешалось передавать лишь шифровки с дезинформацией.

В то же время итальянские войска начали передавать по радио зашифрованные обзоры боевой обстановки. Особенно этим страдал командующий 1-й армией генерал Пекори-Джиральди. Так, например, в течение 1—4 мая путем радиоперехвата была установлена дислокация всех армейских и 20 корпусных штабов из 25, 37 дивизий из 57 и всех кавалерийских дивизий.

Однако вскоре итальянцы стали пользоваться радиосвязью только в самых экстренных случаях. Все же, благодаря приказу начальника итальянской радиослужбы полковника Кардона

об обязательных донесениях радиостанций, австрийская радиоразведка перед началом наступления давала почти такие же богатые результаты, как и раньше на русском фронте. Полковник Кардона даже не догадывался, что сам предупредил противника о предстоящей смене шифра 6 июня.

В последний год войны в «Эвиденцбюро» во главе с Максом Ронге, включая внутреннюю разведку, работало около 300 сотрудников, 50 должностных лиц, 400 агентов полиции, 600 солдат и 600 информаторов.

В 1918 году экономический кризис, сложная обстановка на фронте и распад соседней Российской империи послужили причиной распада Австро-Венгрии. В результате 28 октября была провозглашена Чехословакия, а 29 октября – Государство словенцев, хорватов и сербов.

31 октября в Будапеште произошло вооружённое восстание, и император Австро-Венгрии Карл I потерял контроль над страной. 1 ноября была провозглашена Западно-Украинская народная республика, а 6 ноября – Польша. В тот же день Карл I отрёкся от престола, и Австро-Венгрия прекратила своё существование.

Несмотря ни на что, австрийская радиоразведка продолжала свою кропотливую работу. Даже 1 ноября было обработано 65 зашифрованных итальянских радиogramм и были правильно установлены группировки и направление движения итальянских армий. Лишь 3 ноября 1918 года, после заключения перемирия, австро-венгерская разведывательная служба вместе со своей радиоразведкой прекратила свою деятельность.

### 3. Радиоразведка Швеции

Начиная с лета 1928 года, радиоразведка в Швеции велась только ВМС и то нерегулярно. Ведение радиоперехвата было возложено на боевой корабль «Sverige», однако с лета 1929 года к решению задач радиоразведки были дополнительно привлечены несколько кораблей из состава сил охраны военно-морских баз, а с октября того же года радиоразведка стала вестись и с береговых узлов связи.

В начале 1930-х годов командование ВМС Швеции предприняло дополнительные меры, направленные на повышение роли радиоразведки. По его инициативе в 1930—31 годы были организованы курсы по подготовке специалистов в области криптографии и криптоанализа. На курсы, которые действовали вплоть до 1935 года, принимались действующие офицеры, а также призванные на военную службу студенты и офицеры запаса. Несколько позднее на курсах стали обучаться криптоанализу гражданские специалисты университета Упсала. Помимо изучения теоретических основ криптологии слушатели курсов получали хорошую практическую подготовку по дешифрованию реальных материалов радиоперехвата. Начиная с весны 31-го, корабли ВМС Швеции с выходом на дозорную службу вблизи побережья страны стали осуществлять регулярный перехват радиопередач кораблей и узлов связи иностранных государств. С целью повышения профессиональной подготовки были организованы постоянные тренировки радиооператоров на корабле «Drottning Victoria».

В 1936 году правительство Швеции, учитывая сложную международную обстановку, приняло решение об очередном реформировании вооруженных сил страны. Планами военной реформы предусматривалось изменение организационной структуры и увеличение численности частей военно-воздушных сил, введение должности верховного главнокомандующего и образование Объединенного штаба, на который возлагались задачи по управлению всеми видами вооруженных сил страны. В рамках проводимой реформы произошли изменения и в организации военной разведки. С 1 июля 1937 года в составе Министерства обороны Швеции начали работу 3 новых отдела – разведывательный, радиоразведки и криптологии.

Формально ответственность за организацию радиоразведки была возложена на управление связи штаба вооруженных сил, однако на практике задачи радиоразведки по-прежнему решались кораблями и подразделениями ВМС – единственного вида вооруженных сил Швеции, располагавшего подготовленными радиооператорами и специалистами радиоразведки.

В состав отдела криптологии вошли 4 секции, три из которых отвечали за обеспечение криптографической безопасности систем связи соответственно сухопутных войск, ВВС и ВМС, а четвертая секция должна была заниматься вопросами криптоанализа шифров и кодов иностранных государств. Все работы отдела предписывалось осуществлять в обстановке глубокой секретности, для чего под его нужды было выделено небольшое, но отдельное здание, которое среди сотрудников стало именоваться «Серым домом». Накануне Второй мировой войны численность отдела возросла, в связи с чем ему были предоставлены помещения на одном из этажей Военной академии. Вскоре и этих помещений оказалось недостаточно, поэтому при очередном увеличении численности сотрудников секция криптоанализа была переведена из академии в отдельное здание.

Утром 30 ноября 1939 года войска Ленинградского военного округа под командованием генерала К. Мерецкова пересекли советско-финляндскую границу и стали продвигаться вглубь Финляндии, что фактически означало начало войны. В тот же день Президент Финляндии Кюёсти Каллио заявил, что «Финляндия объявляет состояние войны».

Именно в годы этой войны, вошедшей в историю как советско-финская кампания или Зимняя война, началось сотрудничество Швеции и Финляндии в области радиоразведки и криптоанализа. Наряду с отправкой добровольцев и поставками вооружения Швеция пере-

давала своему соседу разведывательные данные, полученные путем радиоперехвата и чтения шифр переписки сухопутных частей Красной Армии. Шведским криптоаналитикам удавалось также дешифровать радиотелеграфные сообщения советских ВВС. Многие из них содержали приказы о нанесении бомбовых ударов по столице Финляндии. Очень часто эти криптограммы дешифровывались еще до момента вылета советских бомбардировщиков с аэродромов, расположенных в Латвии и Эстонии всего в 20 минутах полета от Хельсинки. Благодаря этому, финские власти имели достаточный запас времени, чтобы заблаговременно предупредить население города о готовившихся воздушных налетах.

Зимняя война продолжалась 105 дней и завершилась подписанием 12 марта 1940 года мирного договора в Москве. Однако важные события во взаимодействии разведслужб Швеции и Финляндии были еще впереди.

9 апреля 1940 года немецко-фашистские войска вторглись в Данию и Норвегию. В ходе проведения Германией морской десантной операции норвежскими средствами береговой обороны были уничтожены 7 немецких транспортных судов, на борту которых находились войска и вооружение, в том числе и различная техника связи.

Испытывая трудности в организации управления войсками, находившимися на территории Норвегии, Германия обратилась к правительству нейтральной Швеции с запросом об использовании ее линий телефонной и телеграфной связи, проходивших по западному побережью страны.

Получив согласие, командование немецких войск уже с 18 апреля приступило к их использованию. Помимо этого Германия продолжала передачу дипломатических сообщений по отдельной линии, связывавшей немецкое посольство в Стокгольме с Берлином, а начиная с середины июня 1941 года приступила также к использованию новой линии связи Стокгольм – Гельсингфорс. Всего в годы войны в интересах Германии использовались 4 линии телеграфной связи из Осло в направлении Нарвика, Стокгольма, Копенгагена, Берлина и Тронхейма.

Испытывая несмотря на нейтралитет тревогу за безопасность своей страны, военно-политическое руководство Швеции решило не упускать уникальный шанс оказаться в курсе планов немецкого военного командования. В результате уже в конце апреля 1940 года шведская радиоразведка подключилась к доступным ей телеграфным линиям связи и стала осуществлять перехват передаваемых по ним открытых и зашифрованных сообщений.

Одновременно с началом перехвата немецких сообщений шведскими криптоаналитиками была предпринята попытка проникнуть в тайны функционирования немецкой буквопечатающей аппаратуры связи. Результат не заставил ждать себя очень долго – первое представление о принципах шифрования, использовавшихся в машине T-52A/B, было получено секцией криптоанализа уже 25 мая 1940 года. Полученные 27 мая дополнительные материалы перехвата и результаты их анализа подтвердили правильность первоначально сделанных предположений, что позволило уже через две недели сформулировать основные принципы устройства и работы немецкой шифровальной машины.

Основная заслуга в раскрытии шифра принадлежала руководителю группы шведских криптоаналитиков профессору Арне Берлингу. Будущий математик родился 5 февраля 1905 года. После школы поступил в университет Упсала, а по его окончании остался в нем на преподавательской работе. В 1934 году он защитил диссертацию, а в 37-ом стал профессором университета. Научные интересы Берлинга были достаточно широки – отдельные вопросы функционального анализа, теории чисел, теории интегрального исчисления. Перед началом Второй мировой войны Берлинг совместно с группой профессоров, специалистов в области славянских языков и литературы, математики и астрономии, принимал участие в дешифровании закрытого радиообмена кораблей Северного и Балтийского флотов, а также частей Красной Армии. После окончания войны Берлинг в течение 10 лет продолжал трудиться в уни-

верситете Упсала, после чего перебрался в США и длительное время работал в Институте перспективных исследований в Принстоне, штат Нью-Джерси.

Вскоре после того, как Берлингу удалось проникнуть в тайны построения и функционирования немецкой шифрмашин, к работам криптоаналитической секции были подключены несколько технических специалистов во главе с Виго Бергструмом. Им было поручено создание дешифровальных машин в соответствии со схемами, подготовленными группой криптоаналитиков под руководством Арне Берлинга. Уже несколько первых таких машин в значительной мере облегчили и ускорили работу шведских специалистов по взлому зашифрованных немецких телеграмм. Позднее изготовление достаточно большой партии таких машин было налажено на заводе точной механики Эриксона.

Дешифрование немецких телеграмм продолжалось достаточно долго – с июня 1940 по май 1943. Шведские криптоаналитики успешно справлялись с возложенной на них задачей, несмотря на неоднократную смену ключевых процедур и появление на контролируемых линиях телеграфной связи более совершенных моделей немецких шифровальных машин. Перехват сообщений осуществлялся на буквопечатающие аппараты, расположенные в том же здании, где размещалась криптоаналитическая секция. Первоначально использовались аппараты американского производства. Поскольку их число было невелико, а доставка новых аппаратов в военное время из США была затруднена, секцией некоторое время использовались аппараты, предоставленные в ее распоряжение шведской администрацией телесвязи. В результате пострадали шведские телеграфисты, вынужденные на отдельных линиях связи вновь вернуться к старому способу передачи сообщений – с использованием кода Морзе. Вскоре криптоаналитики получили необходимое количество немецких буквопечатающих аппаратов фирмы Siemens.

Поступающие с аппаратов телеграфные ленты наклеивались на специальные бланки и передавались специалисту, отвечавшему за вскрытие шифрключей. Как правило, он ожидал, когда в его распоряжении окажется несколько телеграмм, зашифрованных с использованием одного и того же ключа, а происходило это достаточно часто по причине систематического нарушения установленных правил немецкими операторами.

В связи с плохим качеством и большой протяженностью шведских линий связи прием сообщений сопровождался большим количеством ошибок и нарушений синхронизации, в результате чего принятые телеграммы становились нечитаемыми. Это вынуждало операторов передавать одно и то же сообщение по несколько раз. В отдельных случаях число повторов составляло от 20 до 40. Поскольку процедура установки нового ключа сообщения представляла собой довольно утомительное занятие, операторы шли на сознательное нарушение инструкций и передавали повторное сообщение с прежней установкой ключа. В результате у криптоаналитика оказывалось несколько одинаковых сообщений (отличающихся друг от друга за счет ошибок), зашифрованных одним и тем же ключом. Это и позволяло вначале определить ключ сообщения, а затем прочитать само сообщение с использованием дешифровальной машины.

Несомненно, что работе криптоаналитика предшествовала весьма трудоемкая деятельность его коллег по выявлению суточного ключа и схем коммутации ключевых колес с электромеханическими реле шифрмашин.

Поток сообщений, передаваемых по контролируемым линиям связи, непрерывно возрастал – если в 1940 году было передано только 7100 телеграмм, то в 1941 их число возросло уже до 41400, а в 1942 – до 120800 (из них 101000 шифрованных). В связи с увеличивавшимся объемом работ по дешифрованию телеграмм росла и численность секции криптоанализа – в 1941 году в ней трудилось уже около 500 человек.

До осени 1940 года поток перехватываемых сообщений был невелик. При этом информация, содержащаяся в дешифрованных немецких телеграммах, не вызвала какого-либо беспокойства со стороны военно-политического руководства Швеции – ни командование вер-

махта, ни сам Гитлер не проявляли к Швеции значительного интереса. Это позволило криптоаналитической секции наладить свою работу и отработать порядок взаимодействия сподразделениями штаба вооруженных сил и министерством иностранных дел.

В соответствии с заведенным порядком все дешифрованные сообщения, в которых содержались важные сведения стратегического характера, доставлялись из криптоотдела лично полковнику Карлосу Адлеркройцу – начальнику разведывательного отдела штаба вооруженных сил Швеции. После ознакомления с документами Адлеркройц прибывал с ними на доклад к главнокомандующему вооруженными силами генералу Олофу Торнеллу и начальнику штаба вооруженных сил генералу Акселю Раппе. После этого дешифрованные телеграммы поступали к сотрудникам разведотдела для учета и систематизации содержащихся в них сведений. Телеграммы, содержащие менее важные сведения, поступали в разведотдел сразу же после их дешифрования.

По мере изучения содержащейся в них информации все дешифрованные телеграммы сжигались. Исключение составляли только особо ценные с военно-стратегической точки зрения. Круг лиц, которым было разрешено ознакомление с материалами дешифрования, был ограничен небольшим количеством сотрудников штаба. При этом ознакомление осуществлялось на выборочной основе – информация доводилась только до тех лиц, кому это было необходимо в силу исполнения своих служебных обязанностей.

В министерство иностранных дел и секретную службу Швеции материалы дешифрования отсылались только по личному указанию начальника разведотдела. При этом в МИД материалы направлялись в весьма ограниченном количестве, поскольку Адлеркройц считал, что в этом ведомстве слишком мало внимания уделяется сохранению государственной тайны опасаясь утечки информации.

Однако, благодаря хорошим отношениям МИД с руководством криптоотдела, сложившимся еще при прежнем министре Ричарде Сандлере, сотрудники дипломатического ведомства получали интересующую их информацию «из первых рук». В свою очередь МИД также оказывал специалистам криптоотдела весьма важные услуги, информируя их о важнейших событиях, сведения о которых могли содержаться в зашифрованной переписке немецких дипломатов. Это в значительной степени помогало шведским криптоаналитикам в их работе по дешифрованию перехваченных телеграмм. Адлеркройц был крайне недоволен тем, что часть информации попадает в МИД, минуя его, и в течение длительного времени предпринимал безуспешные попытки подчинить себе отдел криптологии.

Начиная с зимы 1941 года военно-политическая обстановка вблизи Швеции становилась все напряженнее. Уже в феврале руководство третьего рейха зондировало возможность переброски немецких войск и вооружения из Норвегии в Финляндию через территорию Швеции. Однако теперь военное командование и МИД страны имели возможность принимать решения исходя из более объективной оценки происходящих событий. Этому способствовало систематическое получение разведывательных данных относительно состава, дислокации и планов использования немецко-фашистских войск на территории соседней Норвегии. Достоверность получаемых сведений сомнений ни у кого не вызвала.

21 апреля сотрудниками криптоаналитической секции была дешифрована важная телеграмма. В ней содержался длинный перечень немецких воинских частей, которые должны были в ближайшее время начать «передвижение в северном направлении». Вместе с тем, из телеграммы следовало, что немецкое командование не планирует каких-либо действий против Швеции. Сведения подтверждались и дополнялись данными, полученными разведотделом от шведских приграничных воинских частей, таможи, полиции, а также показаниями беженцев, прибывших на территорию страны из Норвегии. Перехваченные и дешифрованные сообщения, которыми обменивался МИД Германии со своим посольством в Стокгольме, также не давали поводов для беспокойства со стороны Швеции.

4 июня было перехвачено сообщение о планируемой переброске крупной группировки немецких войск в северную часть Финляндии с территории Германии и Норвегии в срок до 15 числа того же месяца. Спустя неделю были дешифрованы еще 3 телеграммы, еще раз подтвердившие сделанный шведской разведкой еще в конце апреля вывод о том, что Финляндия примет участие в войне с Советским Союзом на стороне Германии. 16 июня вступила в действие линия связи Берлин-Гельсингфорс, проходящая через Стокгольм. В тот же день шведской разведке из дешифрованной телеграммы стало известно о некоторой активизации немецких войск в финской Лапландии.

Все эти факты свидетельствовали о неминуемом приближении войны. Тем не менее, руководство Швеции, будучи уверенным в том, что предстоящая война ее не коснется, и желая сохранить в тайне такой исключительно ценный источник информации как дешифрованные немецкие телеграммы, решило никаких мобилизационных мероприятий в стране не проводить.

С началом боевых действий немецко-фашистских войск против Советского Союза стал стремительно нарастать поток сообщений, адресованных командованию группировок немецких войск в Осло и Рованиemi. Возросло и количество зашифрованных дипломатических депеш, передаваемых на линии связи Стокгольм-Берлин. Информация, получаемая военно-политическим руководством Швеции в 1941—1942 годах в результате дешифрования немецких телеграмм, становилась все более обширной и подробной. Вместе с тем, она носила в определенном смысле локальный характер, что определялось теми задачами, которые возлагались руководством третьего рейха как на немецкое посольство в Стокгольме, так и на командование немецких войск в Норвегии и Финляндии.

## **Конец ознакомительного фрагмента.**

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.