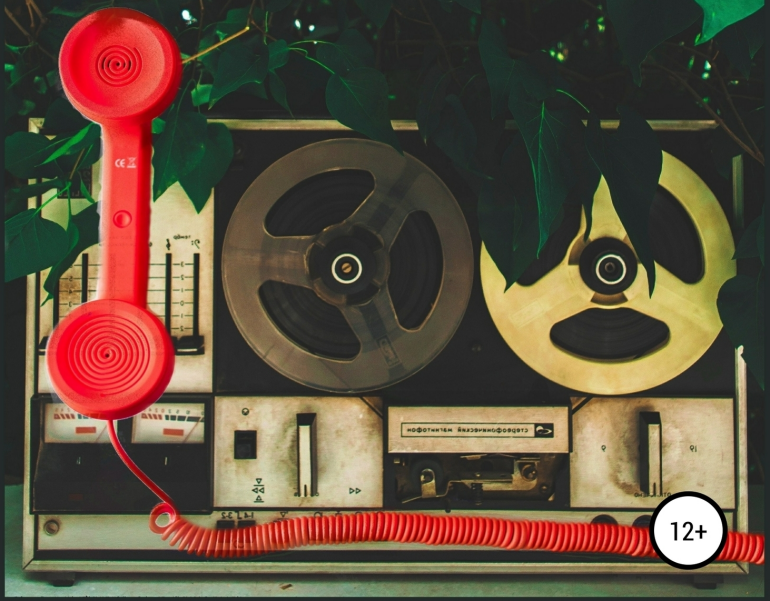
Вадим Гребенников

ПРОСЛУШКА

Перехват информации



12+

Вадим Гребенников

Прослушка. Перехват информации

http://www.litres.ru/pages/biblio_book/?art=39828651
SelfPub; 2018
ISBN 978-5-532-11267-4

Аннотация

Появление негласного контроля какого-либо вида связи всегда связано с рождением этого вида связи. Так, несанкционированное прослушивание телефонных разговоров началось вместе с телефонной связью.Книга рассказывает историю рождения и развития спецслужб, занимающихся прослушкой телефонных разговоров в странах Европы, США, Российской империи, СССР и Российской федерации; создания и эволюции специальной техники оперативно-техническими службами этих стран для контроля телекоммуникаций; описывает наиболее важные спецоперации по перехвату информации и прослушке переговоров.

Содержание

Предисловие

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

Теперь детально рассмотрим тему именно «перехвата» специальными службами в процессе своей секретной деятельности всех видов коммуникаций: проводной и беспроводной (радио) связи.

Спецслужбы испокон веков использовали любые методы и средства, чтобы прослушать и подсмотреть то, что говорят и делают «подозрительные» лица. На заре цивилизации это приходилось делать, находясь рядом с помещением, где находились эти лица, прижимая ухо к двери и подглядывая в замочную скважину или окно.

При выполнении этих функций секретный сотрудник («доброжелатель») подвергался опасности быть пойманным на месте «преступления». Тем не менее, такая работа активно велась спецслужбами, поскольку власть всегда хотела знать, что думают о ней, а главное, что «замышляют» дипломатические представители других государств, политические противники, а также лица, подозреваемые в преступной деятельности.

Кроме государства, такого рода деятельностью занима-

лись и коммерческие организации с целью промышленного шпионажа, и отдельные граждане, чтоб уличить своего супруга (супругу) в измене, а родных или друзей в воровстве. К прослушиванию и подсматриванию иногда добавлялись тайная слежка (наружное наблюдение) и осмотр вещей (негласный обыск).

Можно сформулировать 5 основных задач, которые стоят перед системой «перехвата» коммуникаций:

– контрразведывательная функция: наблюдение за перепиской и деятельностью иностранных дипломатов и иностранцев, борьба с иностранным шпионажем;

– выявление антиправительственной деятельности, обнаружение заговоров и различного рода тайных организаций;

– обнаружение различного рода служебных и экономических злоупотреблений: контрабанда, финансовые нарушения, коррупция; контроль за чиновниками всех уровней;

– изучение реальных настроений различных групп населения;

– обнаружение и изъятие запрещенной в стране литературы, пересылаемой по линиям коммуникаций.

Таким образом, можно сказать, что последние 4 задачи являются частью системы политического контроля. Сам политический контроль – это система регулярного сбора и анализа информации различными ветвями государственного аппарата о настроениях в обществе, отношении различных его слоев к действиям властей, о поведении и намере-

ниях экстремистских и антиправительственных групп и организаций.

Политический контроль всегда включает несколько основных элементов: сбор информации, ее оценку, принятие решений, учитывающих настроения общественных групп и призванных воздействовать в нужном для властей направлении, а также политический розыск и репрессии при наличии угрозы государству и обществу.

В современном мире при наличии огромного множества видов коммуникаций их «перехват» и прослушка телефонных разговоров являются очень актуальной сферой деятельности спецслужб и состоятельных коммерческих организаций всех стран. Они получают в свое распоряжение огромное количество информации как о личной жизни граждан, так и многие детали их деятельности в коммерческой сфере и на государственной службе.

Для того, чтобы спецслужба осуществила легитимное подслушивание (далее – прослушка), законодательство любой страны предусматривает судебное решение. По закону любого государства разрешается нарушать право гражданина на тайну личной жизни и телефонных разговоров только в том случае, если суд признал это необходимым.

Для того чтобы начать кого-нибудь прослушивать, спецслужбе достаточно убедить суд, что этот человек готовится совершить, совершает или уже совершил серьезное преступление. Кроме того, с разрешения суда можно прослушать и

тех, кто сам ничего незаконного не делает, но может что-то знать о преступлении.

В отдельных случаях законодательство позволяет спецслужбе начать прослушку немедленно, а получить судебное решение позже. Такое допускается, если спецслужба обладает разведданными, что готовится какое-то особо крупное преступление или преступление, угрожающее государственной безопасности.

А теперь обо всем поподробнее…

Часть 1. Европейская история

1.1. Прослушка ШКПС

В 1946 году на базе школы в Блетчли Парке была создана Штаб-квартира правительственной связи «GCHQ» (далее – ШКПС) (англ. Government Communications Headquarters). Она обеспечивает планирование, контроль, координацию действий и обработку данных перехвата информации всех разведывательных органов Министерства обороны (ВВС, ВМФ и сухопутных войск) как в стране, так и за рубежом.

Благодаря откровениям бывшего техника Центра безопасности коммуникаций (далее – ЦБК) Министерства национальной обороны Канады Майка Фроста, стало известно, что в 1980-е годы ШКПС по заданию Премьер-министра Маргарет Тэтчер использовал ЦБК, чтобы прослушивать 2-х собственных министров, которые были тогда «оппозиционерами».

Один из прослушиваемых чиновников был министр иностранных дел Фрэнсис Пим, который курировал ШКПС и военную разведку «MI6», а другой – заместителем Премьер-министра и министром внутренних дел Уильямом Уайтлоу.

Нельзя оставить без внимания и заявления американца

Эдварда Сноудена, который с двумя миллионами секретных файлов АНБ сбежал из США и 1 августа 2013 года получил временное убежище в России. Он работал в АНБ, информационном отделе ЦРУ и консалтинговых компаниях, сотрудничающих с АНБ, и имел допуск не только к совершенно секретной, но и специальным разведданным, содержащим технические детали операций США и их союзников по перехвату и прослушке.

Сноуден предал огласке секретную информацию АНБ, касающуюся прослушки телефонных разговоров и перехвата электронных сообщений миллиардов людей из десятков стран. В результате свидетельств Сноудена стало известно о существовании секретных разведывательных программ, используемых в США, Великобритании, Франции, Швейцарии, Швеции, Китае и Индии.

Согласно документов, предоставленных Сноуденом, ШКПС и АНБ с 2005 года перехватывали звонки и данные с мобильных телефонов пассажиров иностранных авиакомпаний. Как говорится в одном из документов АНБ за 2003 год, по оценке ЦРУ, следующими потенциальными целями террористов могут быть рейсы авиакомпаний «Air France» и «Air Mexico».

По утверждению юрисконсультов АНБ, «отслеживание самолетов обеих компаний за пределами США не вызовет юридических проблем». Также указывалось, что «они должны находиться под жестким надзором с момента входа в воз-

душное пространство США».

На борту самолетов «Air France» данные начали собираться в 2007 году, после того, как авиакомпания успешно провела испытания телефонной связи на основе стандарта «GSM» второго поколения.

В 2012 году ШКПС представил программу под названием «Southwinds», предназначеную для сбора данных голосовой связи, передаваемых данных, метаданных и содержания звонков, сделанных на борту воздушного судна. Сбор данных осуществляется в режиме почти реального времени.

Для перехвата содержимого телефона пользователя достаточно двух условий: телефон должен быть включен, а самолет – набрать высоту 3 тысячи метров. Сигнал, проходящий через спутники, затем отправляется на наземные станции прослушки.

Как отмечает издание, сотрудники британской спецслужбы могут удаленно вызвать сбой в работе смартфона, вынуждая владельца повторно ввести код доступа, и перехватить идентификаторы мобильного устройства.

В «Air France» заявили, что на борту самолетов компании не предоставлялись услуги голосовой связи, за исключением тестового периода в 2007 году. В связи с тем, что первое испытание оказалось неудачным, проект был закрыт.

Согласно утверждению Сноудена ШКПС вместе с АНБ осуществляла мониторинг компьютеров и перехватывали телефонные звонки иностранных политиков и чиновников,

участвовавших в саммите «Большой 20-ки» в Лондоне в 2009 году. Во время саммита перехватывались в том числе телефонные переговоры тогдашнего президента России Дмитрия Медведева.

У АНБ есть программа, похожая на «комплект смурфов», на разработку которой был потрачен миллиард долларов. Технология слежки за смартфонами используется спецслужбами против лиц, подозреваемых в терроризме или педофилии.

Программы, которые использовали в АНБ для прослушки телефонных переговоров, умеют автоматически распознавать содержание бесед, переводить их в текстовой формат и записывать так, чтобы их было удобно хранить и находить в базе данных.

5 октября 2015 года Сноуден сообщил, что ШКПС имеет возможность раскрывать мобильные телефоны без ведома пользователя. Для проникновение в смартфон используется отправка специального текстового сообщения, получение которого происходит незаметно для пользователя. Инструменты взлома и дистанционного управления смартфоном называется «комплектом смурфов» (англ. Smurf suite):

– «Мечтательный смурф» (англ. Dreamy Smurf) – инструмент управления питанием, что означает, что ваш телефон можно включать и выключать без ведома владельца,

– «Любопытный Смурф» (англ. Nosey Smurf) – программа активации микрофона телефона без ведома владельца,

– «Смурф-следопыт» (англ. Tracker Smurf) – механизм геолокации, который позволяет спецслужбе отслеживать местоположение смарфтона с большей точностью, чем это возможно путем обычной триангуляции вышек мобильной связи,

– «Параноидный смурф» (англ. Paranoid Smurf) – механизм самозащиты, охраняющий манипуляции смартфоном со стороны спецслужбы.

Кроме ШКПС, прослушкой занимаются и некоторые граждане Великобритании. Так, в 2010 году разразился скандал вокруг того, что Энди Коулсон, советник по связям с общественностью премьер-министра Великобритании Дэвида Кэмерона, прослушивал известных людей. Коулсона обвиняли в том, что, когда он был главным редактором популярного таблоида «News of the World», то требовал от своих подчиненных собирать информацию «любой ценой», даже нарушая закон.

В 2007 году один из корреспондентов этого издания попал за решетку на 4 месяца за прослушку. Тогда было доказано, что он организовал прослушку голосовой почты членов королевской семьи Великобритании. Из-за этого случая Коулсон был вынужден уйти из редакции, но ему удалось избежать наказания за прослушку, поскольку его вину не удалось доказать. Он утверждал, что не знал о происходящем в редакции.

В 2005 году в британской королевской семье отмечали,

что непрочитанные сообщения и не прослушанные записи голосовой почты внезапно изменяли свой статус на «прочитанные». Тогда в прессе начали появляться новости из частной жизни наследника престола Великобритании принца Уильяма.

С разоблачением о прослушке выступил Шон Хор, один из бывших репортеров «News of the World». По его словам, Коулсон лично предложил ему заняться прослушкой телефонных разговоров знаменитостей. С помощью прослушивания голосовой почты телефонов, а также чтения сообщений «SMS» в телефонах политиков и известных людей издание получало эксклюзивные новости.

После заявления Шона Хора о прослушке, парламент Великобритании создал специальную группу для расследования этого дела. В лондонской полиции сказали, что в списке потенциальных «мишеней» таблоида от 91 до 120 человек. Их имена пока не сообщают. На данный момент полиция обнаружила доказательства 12 случаев совершения уголовного преступления.

Сам Коулсон, который ныне возглавляет службу Кэмерона по связям с общественностью, категорически отрицает такую практику.

«News of the World» получала на протяжении многих лет бульварные эксклюзивные новости о скандальных историях супружеской неверности, бытового насилия, сексуальных оргий и коррупции во власти, прослушивая известных лю-

дей и политиков, утверждают известные издания «BBC», «Guardian» и «New York Times».

1.2. Прослушка 3-го рейха

Многие удивятся, но приход к власти фашистам обеспечили не хорошо вооруженная армия, а массовая прослушка телефонной сети Германии! С согласия Адольфа Гитлера Научно-исследовательский центр «FA» (нем. Forschungsamt) Министерства авиации, которым руководил рейхсминистр авиации Герман Геринг, занимался перехватом и дешифровкой всех телефонных, телеграфных и других систем связи Германии. Под «колпаком» фашистов оказались все известные немецкие политические и профсоюзные деятели, а также представители прессы.

«FA» контролировал телефонную и телеграфную сети, а также радиосвязь. Под пристальным наблюдением находились переговоры немцев с зарубежными абонентами, а также телеграммы, идущие в страну и из страны. «FA» удавалось даже перехватывать обмен сообщениями между иностранными государствами; что касается сношений, идущих транзитом через германские средства связи, они подвергались систематической прослушке и дешифровке.

В пределах Германии прослушивались разговоры влиятельных лиц, как и телефонные беседы известных иностранцев, и, конечно, всех граждан, которые считались политически неблагонадежными, или тех, кто находился под надзором полиции. Прослушка производилась и по случайному

выбору. В случае необходимости институт почти мгновенно мог подключиться к любой линии.

До 1926 года стационарные посты перехвата и прослушки существовали уже в Берлине, Гамбурге, Кенигсберге, Франкфурте-на-Одере, Бреслау, Мюнхене, Штутгарде, Мюнстере и Кёльне. Через 2 года немцы организовали станции перехвата в демилитаризованной Рейнской области под видом гражданских радиостанций.

В дальнейшем численность таких постов и служб радиоперехвата увеличивалась. К 1936 году НИЦ создал развитую сеть центров сбора информации по всей Германии. 12 «исследовательских бюро» и огромная сеть постов перехвата информации как внутри «рейха», так и за рубежом.

Для удовлетворения своих оперативных потребностей «FA» использовал 5 различных типов станций радиоперехвата, называемых исследовательскими центрами. Станции были классифицированы по виду перехвата информации следующим образом: A – телефон, B – радиосвязь, C – радиовещание, D – телеграф, F – почта.

Станции «A» были расположены на станциях телефонной связи Германии, а затем в оккупированных странах. Они были оснащены коммутаторами-перехватчиками, которые позволяли оператору подключиться к любому разговору. В состав каждого коммутатора входил диктофон для записи разговоров. В Берлине была большая станция, на которой работало около 100 человек, используемая для прослушки разго-

воров дипломатического корпуса.

Три станции «D» были расположены в Берлине, Вене и Дортмунде, которые были главными центрами коммутации телеграфных линий, исходящих из Германии.

Станции «F» были созданы после того, как Германия начала Вторую Мировую войну, но их было немного. Результаты почтовой цензуры сообщались «OKW», а затем Главному управлению имперской безопасности «RSHA» (нем. Reichssicherheitshauptamt– Главное управление имперской безопасности). Станция «F» состояла из небольших групп цензоров, прикрепленных к постам почтовой связи.

Помимо станций, действующих в Германии, были созданы оперативные подразделения «FA» в оккупированных странах. В Нидерландах и Польше станции перехвата устанавливались наступающими войсками. В Вене, например, станция «A» начала функционировать через 2 дня после оккупации Австрии.

В каждом телефонном ретрансляторе стояли системы контроля «FA». Основные центры перехвата базировались в Штутгарде, Гамбурге, Мюнхене и Кельне. К 1937 году ежемесячное количество перехваченных телефонных переговоров достигало 50 тысяч и еще 10 тысяч – за пределами Германии.

Каждый день для Гитлера готовились выборки и отчеты о подслушанных разговорах. В то же время любая информация, интересующая министерства и ведомства, немедленно

им передавалась. Однако Геринг, как создатель и руководитель института, всегда имел возможность принять решение о сокрытии некоторых разоблачений и сохранении их в собственных интересах.

Понимая ценность такого инструмента, он стремился сохранить его под своим влиянием и отказался передать в ведение рейхсфюрера «SS» (нем. Schutzstaffel – отряды охраны) Генриха Гиммлера вместе с «Gestapo» (нем. Geheime Staatspolizei – тайная государственная полиция). «Gestapo» и «SD» (нем. SicherheitsDienst – служба безопасности) рейхсфюрера «SS» могли широко пользоваться услугами института, но он до самого конца оставался под контролем Геринга.

Но «Gestapo» тоже умело действовать, устанавливая секретные устройства для подслушивания и записи разговоров в домах подозреваемых лиц. Когда интересующий гестапо субъект отсутствовал или под предлогом ремонта и проверки телефонной линии устанавливались микрофоны, позволявшие шпионить за подозрительными людьми даже в семейной обстановке.

Никто не мог избежать «практики» такого рода. Так, в 1934 году министр правительства Шахт был неприятно поражен, обнаружив в гостиной потайной микрофон. Выяснилось, что его горничная сотрудничает с гестапо, и специальная система позволяет ей прослушивать частные разговоры своего хозяина, даже если ночью он говорит в своей спальне.

Шпионаж стал всеобъемлющим, никто не мог чувство-

вать себя полностью огражденным от него. Генерал авиации Мильх в Нюрнберге рассказывал, что люди боялись не так «SS», как «Gestapo». «Мы были уверены, – сказал он, – что находимся под постоянным надзором; все, независимо от звания. Каждый из нас был занесен в картотеку тайной полиции, и многие немцы попали впоследствии под суд на основе имевшихся там материалов. Вытекающие из этого неудобства касались всех, даже самого рейхсмаршала [Геринга]».

Но особую роль в приходе Гитлера к власти сыграли крупнейшие немецкие промышленники и финансисты, которые изначально недолюбливали фюрера. Сейчас уже известно, что эволюция их политических взглядов явилась результатом всеобъемлющей прослушки всех линий связи, проводимой «FA». Именно компромат на крупнейших банкиров и производственников позволил на определенном этапе «заткнуть им рты» и заставил поддерживать Гитлера в борьбе за власть.

В конце июня 1934 года произошли события под названием «Ночь длинных ножей», когда было ликвидировано немало неугодных людей фашистской партии и ее руководству. Выживших политиков, Гитлер обвинил в измене родине и объявил врагами государства.

Впервые в истории основанием для арестов опять-таки служили компрометирующие записи телефонных разговоров, сделанные на новой для той эпохи звукозаписывающей технике – магнитофоне. Расширение технических возмож-

ностей прослушки в Германии и использование ее результатов для шантажа совпало с началом серийного выпуска магнитной ленты для магнитофона.

В 1934 году фирма «BASF» начала серийный выпуск магнитной ленты на основе карбонильного железа либо магнетита на диацетатной основе. В 1935 году фирма «AEG» выпустила первый коммерческий пленочный магнитофон под названием «Magnetophon K1». Кроме легкой ленты в аппарате присутствовал новый тип кольцеобразных электромагнитных головок.

В 1938 году определилась и классическая троица головок – записывающая, воспроизводящая и стирающая. На стирающую головку подавались токи высокой частоты, в результате чего лента многократно и быстро перемагничивалась. В записывающей головке наоборот была функция дополнительного подмагничивания, снижающая шумы при записи.

Немецкие инженеры разработали уникальные системы прослушки и регистрации телефонных разговоров в сетях стандартных АТС. Эти устройства, установленные в зданиях, где находились АТС, позволяли контролировать одновременно до 1000 абонентов и записывать их разговоры на магнитофоны.

Магнитофон позволял записывать любой (если его сочтут важным) разговор. Для того времени это было поразительное техническое новшество. «FA» систематически регистрировал и помещал в свой архив все телефонные вызовы фю-

рера.

Благодаря мощной финансовый поддержке, новейшим техническим средствам и широкой пропаганде, влияющей на национальные чувства, Гитлер увеличил свою популярность, став фюрером и канцлером. Что касается «FA», обеспечившего новую власть огромным количеством компромата, то он стал непрерывно расширяться и усиливать свое влияние.

15 марта 1938 года была проведена одна из важных операций прослушки в рыцарском замке «Wartburg», где проходило совещание лучших астрологов Германии. Охрану возложили на подразделение «SS» и специальную группу сотрудников радиоразведки гестапо, оснащенной средствами прослушки и новейшими по тому времени магнитофонами фирмы «AEG-Telefunken».

Рейхсминистр Йозеф Геббельс внимательно слушал все, о чем говорили в узком кругу астрологи. К сожалению, почти все записи, да и сами участники того совещания «канули в небытие».

К 1938 году Германия стала мировым лидером по производству специальной техники для разведки. Разнообразные магнитофоны, в том числе и малогабаритные, миниатюрные микрофоны, системы прослушки считались лучшими в мире, ведь они были разработаны в соответствии с последними достижениями немецкой науки в сфере радиотехники и химии.

Первоначально в «FA» работало 4 человека, а к 1942 году ее штат увеличился до 3500 человек. К концу войны количество секретных документов увеличилось в 20 раз. Так, в начале 1935 года в «FA» было зарегистрировано 28 000 документов, а в марте 1945 года их количество составляло уже 425 140! Все это время многочисленные сотрудники «FA» круглосуточно контролировали все кабели связи, проходившие через территорию Германии.

Есть основания считать, что это очень заниженные оценки, так как не учитывалась совместная работа «FA» и Министерства Почты, которое в этом вопросе также подчинялось Герингу. В реальности количество прослушанных телефонных разговоров скорее всего было в 3 раза больше.

Гитлер предоставил Герингу монополию на перехват и прослушку информации, передаваемой по любым линиям связи. Даже всесильный заместитель руководителя «SS» Гиммлера, руководитель «RSHA» Рейнхард Гейдрих, должен был получать специальное разрешение на каждую прослушку телефона. На этом разрешении должен был стоять специальный штамп Геринга «G».

Геринг обладал исключительным правом отключать все телефонные и телеграфные системы связи в стране, кроме линий связи «RSHA». Тотальный контроль за разговорами немцев продолжался все годы нахождения фашистов у власти.

«FA» перехватывало переговоры даже высшего руковод-

ства рейха, Национал-социалистической партии, вооруженных сил, немецких служб безопасности, работников посольств и военных миссий, работавших в Германии. Особый интерес представляли банкиры, а также финансовые и промышленные магнаты. Кроме того, Геринг имел право использовать криптослужбу МИД «Pers-Z».

В его штате состояло около 300 прекрасно подготовленных криптоаналитиков. Для дешифровки информации и быстрых вычислений они использовали даже табуляторы для проведения быстрых вычислений американской компании «IBM» (англ. International Business Machines).

Текст перехваченных телефонных разговоров печатали на особой коричневой бумаге. Документ запечатывали в красный конверт и посылали в сопровождении специального курьера «FA». Каждый такой документ должен был вернуться в «FA», после того как был изучен тем лицом, которому это сообщение было адресовано. Это касалось даже Гитлера. Таким образом обеспечивалась наивысшая безопасность работы.

С разрешения Геринга информация из «FA» поступала в Министерства экономики и пропаганды Германии. В «FA» работали опытные экономисты, прекрасно разбиравшиеся в финансах и экономике. С помощью перехваченной и соответственно обработанной экономической информации специалисты Геринга, возможно, ограбили и разорили многие европейские фирмы и банки, добывая деньги для Германии.

Специалисты «FA» называли полученную в результате перехвата и прослушки информацию «убийственной» из-за силы ее воздействия на политических противников фашистского режима как внутри Германии, так и за ее пределами. В «FA» функционировало особое подразделение, формировавшее специальный компромат на противников фашистского режима на основании прослушанных телефонных разговоров.

Если сравнить численность «FA» с IV управлением «RSHA», она была более, чем вдвое больше. В 1942 году в центральном аппарате IV Управления «RSHA» служило «всего» 1500 человек.

Перехватом информации также занималась военная разведка и контрразведка «Abwehr» (нем. оборона, отражение – от Auslandsnachrichten– und Abwehramt). Так, группа «N» отдела «Abwehr-III» ведала охраной государственной и военной тайны.

Она отвечала за связь с органами службы информации и связи – пресса, кино, почта; в военное время – цензуру и наблюдение за СМИ и почтовыми отправлениями; руководство пунктами цензуры почты и телеграмм из-за рубежа в стране и на оккупированных территориях; организацию и контроль голубиной почты, а также за прослушку телефонных разговоров.

«Abwehr» имел мощный и многочисленный отдел военной цензуры. В его функции входили контроль за частной

и коммерческой перепиской, полевой почтой, обработка писем военнопленных и телеграмм из-за рубежа и т. п. Имелась в отделе и химическая лаборатория. В ней работали первоклассные специалисты, способные проявлять записи, сделанные симпатическими чернилами, перлюстрировать почтовые отправления, защищенные самыми хитроумными способами (вроде прошивания конвертов швейной машинкой), снимать и возвращать на место сургучные печати и т.п.

В 1936 году на совместном совещании с дешифровальным отделом военного министерства «Abwehr» принял решение о реорганизации и укреплении службы перехвата и прослушки с целью подготовки войны против Чехословакии. Во взаимодействии с австрийской и венгерской спецслужбами было осуществлено тайное подключение ко всем кабельным линиям, идущим в Чехословакию и оттуда, вблизи 3-х граничащих с ней стран.

В начале Второй Мировой войны немецкие криптоаналитики могли дешифровать значительную часть шифрованных сообщений, которые передавались по кабельным линиям связи Европы. Этому способствовало то, что множество международных телефонных и телеграфных кабелей проходило по территории Германии.

Анализируя политические шаги Гитлера накануне и в начале войны, можно допустить, что все его действия были обусловлены получением огромного фактического материала, основанного на прослушке и перехвате государственной

и военной переписки стран, которые он планировал аннексировать или захватить.

Вальтер Шеленберг, который в начале 1940-х годов был назначен начальником VI управления «RSHA», пришёл к выводу о том, что для повышения эффективности операций управления нужно, во-первых, установление контроля над всей системой почтово-телеграфной связи Германии за рубежом, а во-вторых, использование перехвата и дешифровки в качестве главного средства разведки и контрразведки.

Интересный факт, до последнего момента в совет директоров американской компании «ITT» (англ. International Telephone and Telegraph) входили глава фашистской политической контрразведки Вальтер Шелленберг и командующий немецкими сухопутными войсками связи генерал Фриц Тиле, который до назначения на эту должность возглавлял радиоразведку «вермахта». Неудивительно, что немецкая разведка раздобыла алгоритмы шифрования и ключи к «скремблеру», сделанному компанией «ITT».

Наиболее успешной операцией был перехват закодированных «скремблером» (англ. scramble – шифровать, перемешивать) радиотелеграфных разговоров высших руководителей США, в том числе Президента США Франклина Рузвельта, с их коллегами на европейском континенте. С осени 1941 года перехват за пределами Германии осуществляла база Исследовательского института германского имперского почтового ведомства в Голландии.

Две мощные направленные антенны ромбовидной формы располагались на побережье около Нордфолка. Они круглосуточно прослушивали англо-американские радиотелефонные переговоры, закодированные «скремблером» А-3, разработанным компанией «ITT». Немецкий радиопост ежедневно перехватывал более 60 телефонных переговоров.

В результате немецкой дешифровальной службе удалось в 1941 году раскрыть принцип засекречивания телефонных разговоров в системе А-3. Это позволило немецкой разведке регулярно получать дешифрованные записи переговоров, которые вели Президент США Ф.Рузвельт, Премьер-министр Великобритании В.Черчилль, Министр иностранных дел Великобритании А.Иден, помощник Президента США Р.Гопкинс, американский генерал М.Кларк и другие.

Переведённые с английского на немецкий язык тексты дешифрованных переговоров высокопоставленных лиц США и Великобритании докладывались командованием немецкой разведки непосредственно Адольфу Гитлеру, а также другим руководителям «третьего рейха».

Стоит заметить, что во время Второй Мировой войны деятельность немецких телефонных компаний по перехвату информации государственных и коммерческих организаций простиралась вплоть до Латинской Америки, контролируя практически все страны этого континента, что позволяло «кригсмарине» проводить успешные боевые действия в этом регионе.

За годы прослушки фашисты накопили огромное количество компромата на ведущих политиков по всему миру. К сожалению, эти секретные данные помогли многим из нацистов избежать после окончания войны заслуженного наказания и долгие годы успешно скрываться в странах Южной Америки и Ближнего Востока, где у власти находились люди, «запачканные» сотрудничеством с верхушкой «третьего рейха».

В Третьем Рейхе существовал также специально оборудованный «бордель» для нацистской верхушки и важных иностранных гостей. Так называемый салон Китти находился в Берлине-Шарлоттенбурге на Гизебрехтштрассе, 11. На протяжении 1939–42 годов его курировала служба безопасности рейхсфюрера «SS».

Идея создания борделя для общественных деятелей, дипломатов и высокопоставленных нацистских функционеров принадлежала руководителю «RSHA» Гейдриху, а в жизнь ее воплотил Шелленберг. В стены борделя были встроены микрофоны, а в подвале была оборудована центральная станция, с помощью которой осуществлялась прослушка и запись разговоров.

Специалисты по техническим средствам прослушки сделали все необходимое: двойные стены, современная аппаратура и автоматическая передача информации на расстояние. Все это позволило фиксировать каждое слово, произнесенное в этом салоне, и передавать его в Центральное управле-

ние.

К тому же Шелленберг отобрал 20 женщин легкого поведения, которые должны были интеллигентно выглядеть, знать несколько иностранных языков, разделять националистические убеждения и обладать ярко выраженными склонностями к нимфомании. Они проходили комплексное обучение шпионажу, чтобы как можно полнее «обработать» своих собеседников.

Посетитель должен был взять номер, расположиться в нем, и только после этого к нему приходила девушка. Кстати, девушки салона не знали о подслушивающих устройствах. Но каждый вечер, после того как «закончен бал и погасли свечи», все они – хозяйка не была исключением – писали подробные отчеты, с которыми затем сравнивались результаты звукозаписи.

Создание салона в оперативном отношении оказалось в высшей степени успешным. В результате прослушки и тайного фотографирования служба безопасности имела возможность значительно пополнить свои досье ценной информацией. Ей удавалось, в частности, выходить на скрытых противников нацистского режима, а также раскрывать планы прибывающих в Германию для переговоров представителей разных стран.

Среди тех, кого таким образом прослушали, были, к примеру, министр иностранных дел Германии Иоахим фон Риббентроп, министр иностранных дел Италии Галеаццо

Чиано, а также оберстгруппенфюрер «SS» Йозеф (Зепп) Дитрих. В салоне Китти проверяли, прежде всего, верных национал-социалистическому режиму функционеров. В 1942 году в дом, в котором находился салон Китти, попала авиабомба, и вскоре после этого он был закрыт службой безопасности «SS».

В первые годы после войны стала известна подробность, ставшая поистине ударом для Вальтера Шелленберга. Частый гость салона, пресс-атташе посольства Румынии Любо Колхев, оказался британским разведчиком Роджером Вильсоном. Вильсон выбирал все время одну и ту же девушку, которую ему удалось перевербовать. Мало того, он заметил 3 кабеля, ведущие в подвал, и даже сумел подсоединить к ним свои «жучки». В итоге британская разведка имела полную возможность знакомиться с результатами прослушки.

1.3. Тотальный контроль «Stasi»

В апреле 1950 года в ГДР была создано Министерство государственной безопасности (нем. Ministerium fur Staatssicherheit), сокращённо – «Штази» (нем. Stasi). К середине 1952 года «Stasi» фактически управлялась исключительно советскими генералами и офицерами. Её структура и деятельность с самого начала были построены также, как и в КГБ СССР.

Одним из наиболее важных и особо секретных направлений деятельности «Stasi» являлось масштабная телефонная прослушка, с помощью которой руководство ГДР оперативно получало достоверную информацию о настроениях и лояльности населения страны, а «Stasi» быстро выявляло диссидентов и враждебно настроенных лиц, тщательно изучало все стороны личной жизни как своих граждан, так и иностранцев с целью вербовки и последующего использования в качестве уже собственных агентов.

В 1954 году в «Stasi» было создано подразделение для контроля телефонных переговоров, преобразованное год спустя в самостоятельный отдел. В 1960 году он получил название, под которым просуществовал до самого конца – отдел «26». С середины 1970-х годов на него были возложены в большей степени контрразведывательные задачи, обозначенные как «Задание X».

К задачам относились активные и пассивные и мероприятия, от установки защищенных от прослушки телефонов и использования специальных приборов для установки помех, мешавших противнику прослушивать разговоры до контроля телефонов, владельцы которых вызывали подозрения.

Масштабы прослушки телефонов, наконец, возросли настолько, что в Восточном Берлине все абоненты открытой телефонной сети при необходимости могли прослушиваться и одновременно записываться до 2-х тысяч телефонных переговоров. Первое было возможно лишь потому, что в Восточном Берлине на 100 жителей приходилось в начале 1980-х годов лишь 4 телефона (в ФРГ в то же время – 43).

20 лет отдел «26» следил за телефонными звонками на Запад, но в 1983 году эта задача была передана 3-му главному отделу (радиоперехват и радиотехническая разведка) МГБ. Тем самым в организационном и техническом планах деятельность «Stasi» по контролю телефонных звонков внутри ГДР и из ГДР в ФРГ была разделена.

Если 3-й главный отдел, в котором работали 6 тысяч штатных сотрудников, прослушивал беспроводную связь, радиопереговоры, связь со спутников и автомобильных телефонов, а теперь и зарубежные звонки с телефонов и телефаксов, то отдел «26» по-прежнему отвечал за проводную телефонную связь в самой ГДР.

Впрочем, использование этого отдела в контрразведывательных целях возросло. Так, в 1980-х годах отдел «26» по-

лучал большинство запросов на прослушку от 2-го главного отдела (контрразведка) МГБ, например, в 1985 году – 299 запросов на прослушку телефонов и 59 на прослушку помещений, причем это количество почти удвоилось в сравнении с началом десятилетия.

В течение многих лет сотрудники Менхена подключились к 2200 телефонам американских учреждений, находящихся в Западном Берлине. Чтобы яснее представить размах этой операции, нужно подсчитать, сколько же требуется персонала, чтобы круглые сутки прослушивать половину этого количества. Прослушивание второй половины телефонов было компьютеризировано. Телефонные разговоры записывались автоматически, после чего хранились для последующего анализа.

За прослушку и телефонный контроль на территории ГДР в «Stasi» отвечал 26-й отдел, который должен был обеспечить работу собственных подразделений в каждом из 15 округов страны. Офицеры отдела вели контроль за 4000 телефонных номеров централизованно и до 1500 – на окружных постах. Ежегодно проводили до 900 мероприятий прослушки.

Для обеспечения бесперебойной работы только этих подразделений «Stasi» требовалось огромное количество надёжных магнитофонов с высоким качеством записи, в связи с чем, оперативные и технические службы, наряду с разработкой собственной аппаратуры звукозаписи, активно исполь-

зовали импортные модели.

В 1956 году Оперативно-технический сектор «Stasi» начал разработку системы телефонной прослушки, названной как «Система-А», которая активно использовалась уже в начале 1960-х годов. Система базировалась на современных для того времени ламповых и релейных компонентах, а в качестве аппаратуры звукозаписи применялись как собственные, так и импортные ленточные (бобинные) магнитофоны.

При этом разработчики системы использовали отдельные технические решения, реализованные американским ЦРУ и британским «MI6» в операции «Gold», которая была раскрыта и внимательно изучена специалистами «Stasi» и КГБ. В ходе этой операции под границей Западного и Восточного Берлина был тайно прорыт и оборудован 500-метровый тоннель, где в течение года сидели западные специалисты для обслуживания многочисленной аппаратуры прослушки советских подземных военных телефонных кабелей.

В «Системе А» при поступлении задачи на контроль определенного телефонного абонента офицеры «Stasi» технически могли подключаться к его разговорам в самых разных узлах связи. Это делалось конспиративно на центральном или дополнительном распределительном щите каждой АТС или в разных местах прохождения кабельной сети (около 70% в местах перемычек, около 9% на линейных распределителях, примерно 19 % на кабельных разветвителях или в телефонных шкафах, около 1% в других местах).

Во второй половине 1960-х годов МГБ разработала централизованную систему телефонного контроля под кодовым названием «СЕКО» (нем. Centrales Kontrollsystem). Эта система оборудовалась постепенно и с 1973 года стала использоваться на постоянной основе. В «СЕКО» применялась техника на гибридных и дискретных транзисторных компонентах, а также магнитофоны «Jesenik» и «Hostyn» чехословацкого производства, размещенных в вертикальных стойках.

В качестве носителя информации использовался оригинальный картридж, позволявший быструю замену при окончании магнитной ленты. Эти магнитофоны были специальной продукцией и выпускались только для потребностей подразделений государственной безопасности.

При этом обеспечивалось время записи до 90 минут. На практике эти магнитофоны требовали постоянного квалифицированного обслуживания, и в МГБ было принято решение в дальнейшем разрабатывать и производить свое собственное оборудование звукозаписи.

Система «СЕКО» была разработана таким образом, чтобы обеспечивать централизованное прослушивание до 4000 телефонных номеров и до 1500 номеров локально, с помощью временных и передвижных постов контроля. В Берлине «СЕКО» содержала до 1100 блоков-стоек телефонного контроля.

Своей высокой производительности «СЕКО-2» достигала, во многом, благодаря подземным коммуникациям в Бер-

лине, которые были построены еще при Гитлере и во многом смогли сохраниться во время войны.

В общей сложности «СЕКО» давало возможность контролировать до 0,3% из 1,8 миллионов телефонных абонентов ГДР. Система обеспечивала не только перехват и запись телефонных переговоров (мероприятие «А»), но и контроль и запись разговоров в помещениях с помощью техники прослушки (мероприятие «В»). При этом использовалось как низкочастотное оборудование для ввода информации на контрольную стойку «СЕКО», так и высокочастотное, для передачи информации «на поднесущей частоте».

В секретных документах МГБ также использовались следующие термины:

– мероприятие «V» – контроль телекоммуникационных сетей;

– мероприятие «R» – контроль телексной связи и передач с цифровой модуляцией;

– мероприятие «L» – контроль радиорелейной и спутниковой связи.

В начале 1980 годов началась модернизация системы «СЕКО» и замена на технику с новыми компонентами. Появилась собственная аппаратура звукозаписи и таймирования, изменились процедуры прямой коммутации. В «СЕКО-2» использовались транзисторы и интегральные схемы, а также собственные кассетные магнитофоны «CAG» и позднее «CAW-E» производства завода ГДР «Elektronik».

О масштабах технической оснащенности «Stasi» свидетельствовало то, что в 1989 году использовалось около 12 тысяч этих магнитофонов. Кассеты прослушивались на отдельных рабочих местах и при необходимости информация переносилась на бумагу.

Центральные базы системы «СЕКО-2» располагались в 15 окружных управлениях и отделах МГБ. В Лейпциге, например, это было здание «Runden Ecke», где в настоящее время находится музей «Stasi» с бункером «СЕКО-2». В Восточном Берлине центральная база системы располагалась в районе «Johannisthal».

Технические узлы «СЕКО-2» располагались в 209 территориальных подразделениях МГБ и были соединены кабелями с окружными управлениями МГБ. Интересно, что в системе использовались дополнительные кабели и трассы коммуникаций, которые сдавались в аренду Министерством Почт ГДР для использования в интересах «Stasi».

В Восточном Берлине находилось 18 базовых станций «СЕКО-2», связанных по кабелю с ближайшими телефонными станциями. Система позволяла одновременно прослушивать 400 тысяч переговоров при общем числе телефонов в ГДР 8 миллионов.

Столь большое количество станций объяснялось наличием в этой части Берлина значительного количества объектов оперативного интереса «Stasi», таких как, иностранные посольства и торговые представительства, государственные

учреждения, крупнейшие гостиницы и многое другое.

Специальные кабели от станций «СЕКО-2» поступали на главный распределительный щит ближайшей АТС и через них нужные для МГБ абоненты подключались к системе. 70% подключений производилось на главном распределительном щите, 9% на линейных распределителях, 19% на кабельных разветвителях или в шкафах, 1% в других точках.

От базовых станций информация передавалась через кабели на Центральную базовую станцию в районе «Johannisthal». При этом определенная часть данных прослушки передавалась с помощью высокочастотной модуляции (на поднесущей частоте), а также с цифровой модуляцией для передачи многоканальной телефонной связи.

На базовой станции «СЕКО-2» по улице «Frankfurter Allee» располагались рабочие места, где офицеры МГБ вели непосредственную прослушку телефонных переговоров, которые по разным причинам не могли быть записаны.

На центральной берлинской станции «СЕКО-2» располагались 4 стойки общим количество 1100 контрольных точек подключения, а также 20 индивидуальных постов в отдельном помещении для работы офицеров МГБ.

Контролируемые МГБ переговоры записывались на кассетные магнитофоны. При этом на 1-ую дорожку записывалась основная информация, а на 2-ой дорожке отмечались дата, время и телефонный номер вызываемого абонента. Интересно, что номер вызывающего абонента не определялся.

За период 1960–89 годов телефонная прослушка трижды модернизировалась и постоянно оснащалась современной аппаратурой производства ГДР. Кроме того, с помощью разветвленной кабельной сети специалисты «Stasi» могли быстро организовать акустический контроль самых разных помещений, от частных квартир и коттеджей, до номеров современных гостиниц, офисов иностранных представительств и государственных учреждений.

После объединения ГДР и ФРГ вся техника «СЕКО-2» была отключена и уничтожена вплоть до отдельных магнитофонов. Только на станции «Runden Ecke» в Лейпциге остались несколько образцов аппаратуры системы прослушки в качестве музейных экспонатов.

По данным бывших сотрудников контрразведки между 1977 и 1986 годами «Stasi» почти 50% всех первоначальных «наводок» на западных шпионов в ГДР получало от неофициальных сотрудников и с использованием средств и методов из так называемой «оперативной области», т.е. в ФРГ. Чуть больше 30 % приходилось на сведения, полученные с использованием прослушки телефонных переговоров и перлюстрации почты в самой ГДР.

1.4. Контроль в Германии

27 сентября 1950 года в ФРГ была создана контрразведывательная спецслужба – Федеральное управление по защите Конституции «BFV» (нем. Bundesamt for Verfassungsschutz), которое обеспечивало функционирование систем секретной связи и информации, а на его 1-й отдел было возложена прослушка телефонных разговоров.

В 1955 году в ФРГ была создана Федеральная разведывательная спецслужба «BND» (нем. Bundesnachrichtendienstes), которая обеспечивала получение информации с каналов связи с помощью технических средств, а раскрытие шифров было возложено на её 2-й отдел (техническая разведка), в котором сейчас работают 1,5 тысячи сотрудников.

В данный момент «BND» и «BFV» совместно с ЦРУ США осуществляют глобальный проект видеонаблюдения «Проект 6» (англ. Project 6) с целью борьбы с терроризмом. Он включает массивную базу данных, содержащую такую личную информацию, как фотографии, номера номерных знаков, истории поиска в интернете и телефонные метаданные предполагаемых террористов.

Эти немецкие спецслужбы также осуществляют слежку за своими гражданами в интересах США при содействии и непосредственном участии АНБ. Разработанная американ-

цами программа «X-Keyscore» позволяет им ежемесячно получать данные о 500-х миллионах контактов немецких граждан, включая переписку в интернет-чатах, электронную почту, а также телефонные звонки и SMS-сообщения.

Полицейские сегодня пользуются уже довольно большим инструментарием в разведывательной области. Сюда входит использование технических средств для прослушки и наблюдения внутри и вне жилищ, перехват телефонных переговоров, мобильной и электронной почты, пеленгация электронных передатчиков, использование видеонаблюдения и даже требования о наблюдении с воздуха или со спутников в рамках межведомственного сотрудничества.

Дополнительные данные, получаемые от телекоммуникаций и об использовании услуг телефонных служб позволяют получать важную информацию о круге общения человека:

– данные о времени соединения и номерах абонентов позволяют опознавать участников террористических сетей и точнее проводить расследования;

– данные о звонках с мобильных телефонов позволяют без наружного наблюдения установить место пребывания звонившего в указанное время.

К тому же местонахождения аппарата и профиль коммуникаций с конкретной «мобилки» дают важные сведения о характере наблюдаемого лица или организации. Поэтому «BFV» имеет право требовать такие данные. Подобные права имеют также военная контрразведка «MAD» (нем. Amt

für den militärischen Abschirmdienst) и «BND».

Некоторыми обязательными для информирования в случае требования данными о телекоммуникационных соединениях и об услугах телефонных служб являются:

– данные о состоянии телефонных счетов, номера карточек, определение местонахождения или вызываемого номера абонента, или идентификацию номеров, с которого и на который звонили, либо конечного устройства;

– дата и время начала и конца соединения;

– данные о клиенте, пользовавшемся услугами телефонных служб и телекоммуникаций;

– конечные пункты постоянных соединений, дата и время их начала и конца.

Для запроса на телефонную прослушку нужно назвать номер телефона. Но в последнее время участники террористических групп все чаще пользуются мобильными телефонами, происхождение которых спецслужбам неизвестно. Потому номера таких телефонов не могут быть установлены даже с помощью владельца телефонной сети. Но если знать номер карточки, то, как правило, выяснить номер соответствующего телефона не составляет труда.

Поэтому «BFV» для выяснения местонахождения аппарата получило принципиальное разрешение использовать устройство под названием «IMSI-Catcher» – уловитель «IMSI» (англ. International Mobile Subscriber Identity) для выяснения номеров карты «SIM» (англ. Subscriber Identity

Module) и телефона и на основе этой информации.

«IMSI-Catcher» позволяет выяснить идентификацию включенного мобильного телефона в зоне действия сети. Идентификация «IMSI» зафиксирована на модуле карты «SIM», которую абонент мобильной связи получает при заключении договора на услуги связи.

С помощью «IMSI» можно не только идентифицировать личность абонента, но и определить номер его мобильного телефона. Для того, чтобы узнать «IMSI» прибор «IMSI-Catcher» симулирует базовую станцию ячейки «радиосот» сети мобильной связи. Включенные «мобилки» в сфере действия этой симулированной базовой станции с картой «SIM» симулированного владельца сети автоматически саморегистрируются на «IMSI-Catcher».

Конец ознакомительного фрагмента.