
Вадим Гребенников
ПРОСЛУШКА
Перехват информации
12+

Вадим Гребенников

# Прослушка. Перехват информации

«ЛитРес: Самиздат»

2018

**Гребенников В.**

Прослушка. Перехват информации / В. Гребенников — «ЛитРес: Самиздат», 2018

ISBN 978-5-5321-1267-4

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.

ISBN 978-5-5321-1267-4

# 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 занимались 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 намерениях 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 воздушное 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 потен-

циальных «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 людей 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 разговоров 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 чувствовать 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 возможностей 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 фюрера.

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 руководства 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 управление.

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» получал 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 использовали 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 туннель, 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 Берлине, 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 кон-

троль 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 американцами 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».

Согласно статьи 10 Основного закона (Конституции) Германии тайна телефонных переговоров и прочей связи является неприкосновенной. Ограничения этой неприкосновенности могут, естественно, быть введены только на основании закона. Это и произошло с помощью так называемого Закона «G-10» (назван так по номеру статьи Основного закона). В нем расписывается, для каких целей секретные службы имеют право проводить мероприятия по прослушке.

Если мероприятие направлено против отдельного подозреваемого и включает круг его общения, оно определяется как «ограничение в отдельном случае» или «индивидуальный контроль». Ограничение основных прав отдельного лица предусматривает наличие серьезных подозрений, что данное лицо планирует, совершает или уже совершило одно из преступлений, указанных в «каталоге преступлений», содержащемся в законе «G-10».

Кроме того, возможны «стратегические ограничения» тайны телефонной связи. Стратегический контроль означает, что контролируются не почта и телефонные переговоры отдельного лица, а коммуникационные линии вообще. Из огромного количества перехваченных разговоров вылавливаются отдельные на основе специфических признаков (например, ключевых слов) и подвергаются анализу.

В своем «постановлении» федеральный министр внутренних дел определяет, в каких сферах может происходить наблюдение и какими областями телефонной и прочей дальней связи оно ограничивается. Это постановление должно быть одобрено контрольной комиссией Федерального собрания «Bundestag» (нем. Bund – федерация, Tag – собрание). В пределах дозволенных этой комиссией рамок федеральный министр может дать приказ на прослушку. Решение о необходимости и позволительности данного приказа, включая использование критериев поиска, принимает комиссия «G-10» парламента.

Для хранения в памяти персональных данных в случае разного рода запросов спецслужбы пользуются объединенной системой хранения разведывательной информации «NADIS» (нем. Nachrichtendienstliches Informationssystem). «NADIS» – это связка баз данных «BFV», Земельных ведомств по охране конституции «LfV» (нем. Landesämter für Verfassungsshutz) и отдела государственной безопасности Федерального уголовного ведомства «BKA» (нем. Bundeskriminalamt).

Эта система позволяет всем подключенным участникам прямое ведение и поиск данных в режиме «он-лайн». «BND» и «MAD» тоже участвуют в пользовании системой «NADIS». В базу данных вносятся лица с «устремлениями, направленными против основ свободно-демократического общественного строя», или в случае с «MAD» – персонифицированные данные военнообязанных.

«NADIS» – это система ссылок на досье с делами. «Сердцем» системы является центральная картотека персональных данных, в которой собраны личные данные и ссылки на соответствующие досье.

Это не система, которая содержит важную информацию по самим делам, а автоматизированное вспомогательное средство для поиска нужных дел (картотека ссылок). Она показывает номер дела соответствующих досье, которые имеются в наличии и для лучшей ориентации содержит персональные данные лица, на которое дан запрос – имя, фамилию, дату и место рождения, гражданство и адрес.

Хотя это и облегчает поиск информации, но если одному из участников «NADIS» требуется сама информация из досье, которая выходит за пределы внесенных в компьютеры личных данных, ему придется идти самым обычным путем – подать письменный запрос по официальным каналам в учреждение, ведущее и хранящее дело. Потому система только в ограниченном виде помогает при расследованиях. Помочь при оценке собранных данных она никак не может.

Если данные о человеке хранятся в системе «NADIS», это вовсе не означает, что он экстремист, террорист или вражеский шпион. Большая часть данных – сведения о людях, которым угрожали организации, применяющие насильственные методы, которые могут представлять конкретный интерес для иностранных разведок и лица, прошедшие проверку безопасности для получения какого-либо допуска.

Неприятные чувства, которые вызывает существование этой информационной системы у общественности, можно в какой-то степени, понять, но они в большой степени неоправданны. «NADIS» – не картотека подозрительных лиц. Если человека вносят в ее базу данных, это не влечет за собой никаких дискриминирующих последствий. На самом деле, по самой своей концепции и своему составу «NADIS» не может ни сделать человека «прозрачным», ни гарантировать «контроль над гражданами».

В начале 2003 года в «NADIS» хранилось 942 350 персонифицированных данных. Из них 520 390 внесенных файлов (52,2 %) представляли собой данные на лиц, прошедших проверку безопасности для допуска в государственные учреждения на федеральном и земельном уровнях, имеющие отношения к вопросам безопасности. В начале 2002 года в системе хранились данные на почти миллион человек.

21 октября 2016 года «Bundestag» принял закон, который предусматривает значительное расширение полномочий разведки «BND». Теперь она сможет следить не только за иностранцами, но и за жителями своей страны. Служба была лишена такого права в середине прошлого века, когда была одержана победа над нацистами.

Предусмотрено и увеличение масштаба прослушки. Раньше «BND» имела право собирать лишь 20% трафика одного из крупных интернет-каналов, теперь же она сможет прослушивать 100% трафика всех интернет-каналов.

Прежде спецслужбы могли прослушивать граждан только в 8 целях, среди которых борьба с терроризмом, киберпреступность и незаконная торговля людьми. Закон расширил цели, к примеру, прослушивать граждан Германии с целью сбора сведений внешнеполитического значения. Помимо сбора данных, полномочия «BND» расширены и в вопросах сбора метаданных телефонов.

Поводом для проверки сообщений теперь могут стать не чёткие формулировки о подозрениях в терроризме и т. д., а размытые определения о сведениях, «имеющих значение с точки зрения политики безопасности». Критики считают, что это позволит прослушивать практически любого.

Помимо сбора данных, документ предусматривает, расширение полномочий «BND» и в вопросах сбора метаданных (например, кто с кем говорил, когда и как долго, с какого именно телефона и где в этот момент находился). Теперь для этого не понадобится иметь какие-либо основания – в категорию потенциально прослушиваемых попадут все, кого «нельзя однозначно идентифицировать как граждан Германии».

Критики считают, что такая формулировка оставляет возможности для сбора информации практически о любом человеке. Напомним, согласно исследованиям учёных Стэнфорд-

ского университета, метаданные способны рассказать о человеке настолько много, что прослушка и наблюдение устанавливать за ним в некоторых случаях и не нужно.

Плюс к этому, при «двухпрыжковом» методе сбора метаданных, за ним потянутся метаданные ещё около 25 тысяч абонентов, которые могу быть вообще никак с ним не связаны, но, тем не менее, их личная тайна может стать доступна спецслужбам. «Один прыжок» означает, что подозреваемый А вызывает человека Б, а «второй прыжок» – человек Б вызывает человека В.

## 1.5. Прослушка в Румынии

«Секуритатэ» (рум. Securitate – безопасность) – Департамент государственной безопасности МВД Социалистической Республики Румыния, сочетавший функции спецслужбы и политической полиции.

Он было учрежден 30 августа 1948 года при поддержке спецслужб СССР, а распущен в декабре 1989 года, вскоре после казни президента Румынии Николае Чаушеску.

В 1954 году в составе «Securitate» был создан Генеральный директорат технических операций «DGTO» (рум. Directia Generala de Tehnica Operativa) при поддержке советских специалистов. Он занимал ведущее положение в Департаменте госбезопасности и вел наблюдение за всеми видами телекоммуникаций, прослушивал общественные учреждения и частные дома.

Румынская тайная полиция была настолько вездесущей, что в итоге превратилась в своего рода «пугало»: ее и без того достаточно большая власть многократно увеличилась в воображении румын. Как-то раз в середине 1980-х годов Мариану Челак (известную диссидентку и архитектора) привезли на большой завод, чтобы наглядно продемонстрировать сыскные способности охранки. Все телефонные разговоры записывались на пленку, и в качестве доказательства ей представили кассету под номером 6432.

Главный абсурд состоял в том, рассказывала она, что, хотя они действительно записывали все разговоры, никто очевидным образом этими разговорами больше не интересовался и не анализировал их содержания. Одного знания, что все записывается и прослушивается, оказалось достаточным, чтобы превратить людей в трусов. Инструментом «Securitate» было обычно человеческое чувство страха.

После 1991 года Парламент Румынии реорганизовал спецслужбы, из которых технической разведкой занимается Служба специальной связи «STS» (рум. Serviciul de Telecomunicaţii Speciale). Она отвечает за обеспечение радиоэлектронной разведки и защиты правительственной связи, в том числе и в военное время.

В 1996 году один из сотрудников Румынской службы информации «SRI» (рум. Serviciului Roman de Informacii) капитан Константин Букур обвинил ее в незаконной прослушке телефонов многих политиков и бизнесменов. По его словам, под колпаком спецслужбы среди прочих находились самый богатый бизнесмен Дан Войкулеску, диссидент времен Чаушеску и противник нынешнего режима Дойна Корнеа, а также видный политик и лидер оппозиции Корнелиу Копосу, скончавшийся в 1995 году.

Капитан Букур утверждает, что в его распоряжении имеется не менее 10 кассет с нелегальными записями, сделанными сотрудниками подразделения контроля телефонной связи и записи «Т» военного отдела «SRI», в котором он сам служил. Обнародовать информацию о собственном подразделении он решился из-за того, что госбезопасность нарушает закон, регламентирующий ее деятельность и запрещающий использование ее сотрудников в политических целях.

Капитан обвинил директора «SRI» Вирджила Мэгуряну в использовании методов работы, которые наносят вред национальной безопасности. Возможно, выступление мятежного офицера не имело бы широкого резонанса, если бы его не поддержал лидер партии «Великая Румыния» сенатор Корнелиу Вадим Тудор, политический противник Вирджила Мэгуряну.

Сенатор, прозванный «румынским Жириновским», обвинил шефа «SRI» в том, что он превратил службу госбезопасности в «румынское гестапо». Сенатор провел в своем офисе пресс-конференцию, на которой продемонстрировал журналистам одну из кассет, подлинность которой подтвердили генерал «SRI» в отставке Виктор Марку и один журналист, за которым следит служба госбезопасности.

Главным результатом откровений Букура пока стало решение руководства «SRI» о его увольнении. Одновременно было сообщено о том, что военная прокуратура начала против него следствие. Букура обвиняют в «изъятии служебных документов и незаконном распространении информации в прессе». «Я не знаю, что теперь будет. Возможно, я получу от 2 до 7 лет тюрьмы», – сообщил Букур, добавив, что тем не менее гордится сделанным, хоть и опасается за свою жизнь.

«SRI» и Вирджила Мэгуряну поддержал президент страны Ион Илиеску, который в 1990 году лично назначил последнего руководителем госбезопасности. «Я убежден, что руководство «SRI» не могло позволить себе заниматься тем, в чем его упрекают. Это просто провокация, – заявил глава государства. – Все, кто несет ответственность за подобные провокации или нарушение закона, должны отвечать перед правосудием».

Со своей стороны Букур обвинял власти в том, что они пытаются замять это дело, и пригрозил предать гласности новые доказательства незаконной деятельности «SRI». Его усилия возымели свое действия, и в 1997 году директор «SRI» Вирджил Магуреану подал президенту Эмилю Константинеску прошение об отставке.

После назначения на этот пост в 1990 году его имя связывали в Румынии со всеми громкими скандалами тех лет, что не могло не скомпрометировать «имидж» ведомства. В частности, его обвиняли в незаконной прослушки телефонов многих политиков и журналистов.

Тем не менее, спецслужба тоже сделала свое «коварное» дело, и в 1998 году Букур был приговорен к 2-м годам лишения свободы с отсрочкой исполнения наказания.

Не испугавшись последствий, Букур обратился за защитой в Европейский Суд по правам человека (далее – ЕСПЧ). Суд рассмотрел дело «Букур и Тома против Румынии» (жалоба № 40238/02), в котором обжаловалось уголовное осуждение за разглашение сведений о процедурах прослушивания телефонных переговоров.

8 января 2013 года ЕСПЧ вынес Постановление, что по делу допущено нарушение требований статьи 10 Конвенции о защите прав человека и основных свобод. Суд присудил каждому из заявителей от 7800 до 20 000 евро в качестве компенсации морального вреда. Требование Букура о компенсации материального ущерба было отклонено.

На этом скандалы не прекратились, поскольку в 2007 году стало известно, что Служба внешней информации «SEI» МИД (рум. Serviciul de Informaetii Externe) (внешней разведки) Румынии осуществляла незаконную прослушку телефонов на территории своей страны. Прослушка осуществлялось не в соответствии с судебным постановлением, как того требует законодательство, а только с санкции генерального прокурора.

В связи с возникшим скандалом Председатель Службы Клаудиу Сэфтою подал заявление об отставке румынскому парламенту, проинформировав об этом президента Румынии Траяна Бэсеску. Он признал, что его ведомство вело прослушку телефонных разговоров на территории страны, что не входит в ее компетенцию, однако затем попытался отказаться от своих высказываний.

Несмотря на это, председатель комиссии, председатель Консервативной партии Румынии Дан Войкулеску проинформировал об этом в открытом письме руководство обеих палат парламента, что, в конечном счете, привело к отставке руководителя спецслужбы.

Члены парламентской комиссии пришли к выводу, что румынские спецслужбы обладают техническими возможностями для прослушки любых телефонных разговоров и что их действия вышли из-под контроля парламента.

Отметим, что 39-летний Клаудиу Сэфтою ранее трудился на журналистском поприще. После работы в ряде газет, журналов и на радио он стал советником президента Румынии Траяна Бэсеску по вопросам внутренней безопасности. В октябре 2006 года Сэфтою был назначен на должность начальника разведки. Таким образом он стал вторым журналистом в истории Румынии, который возглавил одну из спецслужб страны.

В 2012 году в Румынии вступил в силу Закон об обязательной регистрации телефонных переговоров, электронной и «SMS»-переписок. Отныне операторы, предоставляющие услуги стационарной и мобильной телефонии, а также интернет-провайдеры будут обязаны создать архив для хранения данных.

Закон предусматривал хранение данных об электронной переписке и содержании телефонных переговоров на протяжении 6 месяцев. Помимо этого, хранящиеся в архивах компаний данные должны предоставляться по первому же требованию представителей правоохранительных и силовых структур Румынии.

Закон действителен как для физических, так и для юридических лиц. Инициаторы принятия этого закона аргументировали необходимость введения такой жесткой меры усилением борьбы с организованной преступностью и терроризмом.

## 1.6. Проект «Энфопол»

Европейский проект «Enfopol» (англ. Enforcement Police – правоприменительная полиция) нацелен на все виды телекоммуникаций, включая компьютерные данные (обычные или шифрованные) и мобильную телефонию (в том числе систему «Iridium» и другие спутниковые системы). Реализация этого плана означает установку слежки за любым видом связи без исключения.

Поскольку сегодня данные между странами передаются очень быстро, «Enfopol» стремится избежать проблем с «нестыковками» в национальных законодательствах и подразумевает контроль за центральной базой проекта «Iridium» в Италии. Однако среди возможных источников информации для европейских полицейских структур называются и компании, предоставляющие международные каналы связи.

Надо отметить, что «Enfopol» (в отличие от проекта «Echelon») – не установившийся порядок, а проект системы сотрудничества между полицейскими силами разных стран. Многие из его параграфов и даже стиль изложения напоминают последние законопроекты, обнародованные (или уже действующие) в Германии и Австрии. Там законопроекты требовали от провайдеров Интернет предоставить правоохранительным органам возможность получать доступ к персональной информации пользователей.

Правительства были вынуждены смягчить формулировки после того, как проекты подверглись жесткой критике со стороны общественности и лоббистских групп (в основном представлявших интересы провайдеров Интернет и телефонных компаний). Сходство проекта «Enfopol» с законодательными инициативами Германии и Австрии означает, что руководители полиции европейских стран пытаются создать гармоничную систему законов по контролю за Интернет в европейском масштабе.

На слушаниях в Европарламенте в сентябре 1998 году всплыли факты сотрудничества между Евросоюза и ФБР, цель которых – построение глобальной системы контроля за телекоммуникациями. Проект «Enfopol» нужно рассматривать именно в этом контексте. Его реализация означает не только всемогущество спецслужб, но и законодательное признание таких систем тотального контроля, как «Echelon».

Официальные лица стараются уделять «Enfopol» как можно меньше внимания. Технические описания мало что говорят большинству простых людей. Написанные на языке крупных телефонных и спутниковых компаний, провайдеров Интернет, тех, кто оказывает услуги другим фирмам, они почти всегда непонятны обычному пользователю Сети.

Требования «Enfopol», регламентирующие контроль за коммуникациями, не могут быть реализованы без серьезного вмешательства в работу действующих коммерческих систем. Не стоит преждевременно обвинять коммерсантов в нарушении права своих клиентов на неприкосновенность частной жизни.

Но если это нарушение станет частью общеевропейской законодательной системы, думается, компании вряд ли 6удут выступать в качестве защитников гражданских прав. Так, немецкие провайдеры воспротивились введению нового закона потому, что на них ложились все расходы по его реализации.

Проект «Enfopol 19» стал результатом встречи руководителей полиции в Брюсселе 11 марта 1999 года и был опубликован 15 марта. Авторы проекта говорят, что «нужды правоохранительных органов… должны быть учтены как в существующих, так и в новых коммуникационных технологиях, в частности, спутниковых коммуникациях и Интернет».

Согласно «Enfopol 19» технические требования 1995 года должны интерпретироваться для применения к Интернет, статической и динамической IP-адресации, номерам кредитных карточек и электронным адресам.

В новом документе подчеркивается, что для контроля за Интернет необязательно собирать данные об отправителе и получателе, так как они включены в каждый пакет данных или IP-пакет. Таким образом, специального регулирования для Интернет не потребуется.

Но это был обманный маневр. Последующие варианты проекта «Enfopol 98» показали, что первоначальный, полный противоречий план, обнародованный журналом Telepolis, был разделен минимум на 5 частей, которые теперь рассматриваются отдельно друг от друга.

Планы контроля за проектом «Iridium» и другими спутниковыми системами связи выделены в отдельный блок и обсуждались на самом высоком уровне в ЕС. Часть проекта «Enfopol 98», где речь идет о сборе персональных данных граждан, будет включена в другие резолюции Евросоюза.

Предполагается, что еще одна резолюция потребует от провайдеров Интернет установить у себя в офисах высокоскоростные системы связи. Эти системы перехвата будут установлены в зоне особой секретности, куда будут иметь доступ только специально отобранные и проверенные сотрудники. Это предложение не вошло в «Enfopol 19».

Если следовать «Enfopol 19», некоторые контролирующие системы будут управляться через «виртуальный интерфейс». По сути это означает установку специального программного обеспечения в точках доступа к Интернет, контролируемого правительственными спецслужбами.

Правоохранительные органы рассчитывают, что предыдущие и новые резолюции сформируют вместе единый пакет, снабженный подробными инструкциями по перехвату сообщений Интернет. Пакет будет включать технические описания, взятые из первоначального проекта «Enfopol 98».

Весьма примечательно, как именно готовился этот проект – в обстановке строгой секретности группой авторов из 20 стран в тесном сотрудничестве с Министерством юстиции США под названием «ILETS». Этот нюанс кое-что проясняет и косвенно указывает «откуда ноги растут».

Это секретная международная организация, возглавляемая США и объединяющая органы безопасности и полиции. Эта организация именуется Международным семинаром правоохранительных органов по телекоммуникациям «ILETS» (англ. International Law Enforcement Telecommunications Seminar) и объединяет сотрудников полиции и государственной безопасности таких стран, как Европа, Гонконг, Канада, Австралия и Новая Зеландия, которые проводят регулярные встречи с начала 1990-х годов.

Организация «ILETS» была создана ФБР в 1993 году после нескольких неудачных попыток провести через Конгресс США новый закон, требующий от производителей оборудования и операторов связи за собственный счет встраивать в аппаратуру средства прослушивания. То, что не получилось сделать в США, стали проводить через международные структуры.

К концу 1990-х годов «ILETS» удалось добиться одобрения своих планов в качестве политики Евросоюза и их включения в национальное законодательство нескольких стран. Впервые эта группа встретилась в исследовательском и учебном центре ФБР в Куантико, штат Вирджиния в 1993 году.

На следующий год они встречались в Бонне и одобрили документ, получивший название «Международные требования по перехвату» (англ. IUR 1.0). В течение следующих 2-х лет требования «IUR» незаметно стали секретной официальной политикой Евросоюза. «ILETS» и его эксперты снова встречались в Дублине, Риме, Вене и Мадриде в 1997 и 1998 годах и разработали новые требования по перехвату Интернета. Результатом же стал документ «Enfopol 19».

Группа лоббирует свои «рекомендации» в европейских правительствах, превращая их таким образом в законы, новые сети и системы связи. Их деятельность никогда не освещается в национальных законодательных собраниях, Европарламенте и даже в Конгрессе США.

В конце концов Европарламент проголосовал за проект «Enfopol» и принял резолюцию о законном перехвате связи в области новых технологий, которая наложила дополнительные обязательства на провайдеров Интернет и других операторов коммуникаций. Эти обязательства включают установку систем мониторинга (в реальном времени) содержимого Интернет, данных о клиентах и об их адресатах.

В соответствии с официальными документами, полиции нужна также возможность определять географическое местоположение владельцев сотовых телефонов, расшифровывать закодированные сообщения (для тех провайдеров, которые предлагают клиентам средства шифрования), осуществлять перехват сообщений, причем все это – в течение нескольких минут или часов.

В резолюции содержится даже требование к провайдерам Интернет предоставлять возможность отслеживать действия пользователя в разных сетях, а также те услуги, которыми он пользуется. Провайдер должен обеспечивать возможность параллельной прослушки пользователя, а результирующие данные должны передаваться правоохранительным органам в читаемом формате.

Ассоциация европейских провайдеров Интернет выразила негативное отношение к резолюции, заявив, что это ошибочное, непроработанное решение.

«Один парламентский комитет проголосовал против предложения, другому не дали возможности высказаться, к тому же голосование проходило в пятницу, когда три четверти членов парламента отсутствовали. Это совершенно неадекватная резолюция», – прокомментировал ситуацию спикер Ассоциации.

Он сказал, что документ вызовет серьезные проблемы в сфере коммуникаций с конституционными гарантиями, и не соответствует законодательству о защите персональных данных.

Европарламент заявил, что резолюция не носит обязательный характер, но в самой резолюции содержится призыв к странам-членам Евросоюза принять соответствующие законы. Дополнение к резолюции гласило, что Евросоюз намерен периодически проверять, насколько страны-члены Евросоюза продвинулись в принятии законов, соответствующих резолюции.

Планы Евросоюза заставить провайдеров Интернет и других поставщиков телекоммуникаций открыть правоохранительным органам доступ к информации клиентов являются неоправданными и нереальными. К такому выводу пришли британские парламентарии на своей сессии.

Комитет по торговле и промышленности Палаты общин, выступивший с отчетом против правительственного законопроекта об электронной торговле, рассмотрел также и принятую Евросоюзом резолюцию.

В своем интервью председатель Комитета Мартин О'Нейл заявил, что в связи с «Enfopol» Комитет опасается появления нереалистичных требований к провайдерам и ухудшения ситуации в области прав человека.

«Мы думаем, что аргументы правозащитников перевешивают аргументы спецслужб, – сказал он. – Если бы они [спецслужбы] четко сказали, каких результатов они хотят достичь, люди, возможно, согласились бы с ними. Иначе все это похоже на прыжки в темноте».

По мнению защитников гражданских прав и провайдеров Интернет, одной ссылки на необходимость борьбы с преступностью недостаточно для того, чтобы спецслужбы получили в свое распоряжение круглосуточный доступ ко всем текстовым электронным сообщениям в реальном времени.

# Часть 2. Американская история

## 2.1. Технологии прослушки

Работа специалистов по прослушке во всех спецслужбах была очень сложной. Они пробирались в подвалы и коллекторы, чтобы уточнить место прокладки телефонных коммуникаций. Им приходилось ходить по подвалам, чердакам и крышам, чтобы под покровом ночи измерить толщину стен нужных зданий. Их посылали в дипломатические миссии, штаб-квартиры компаний, номера гостинниц, в автомобили, самолеты и корабли для установки техники прослушки.

Чаще всего специалистам приходилось работать без всяких графиков, круглосуточно, в любую погоду, без выходных и отпусков. Главное, чтобы был доступ к месту установки прослушивающих устройств. Если тайно проникнуть в посольство можно было лишь после того, как оно закрывалось в конце дня, то рабочий день «слухачей» начинался с наступлением темноты и заканчивался с рассветом.

Оперативная техника, как и методы ее использования, создавались практически с нуля. До 1960 года ее состояние было таким, что все операции по прослушке ограничивались установкой микрофона и прокладыванием кабеля или гальваническим подсоединением к проводам телефонной линии.

Чтобы провести операцию прослушки, необходимо было собрать массу информации: тщательное описание окружения объекта, в том числе мест, подходящих для приема и контроля информации. Потеря сигнала или ухудшение его приема во время испытаний вызывались различными физическими препятствиями.

Любая система охраны и сигнализации, в том числе использование служебных собак, тщательно фиксировалось. На основании собранной информации оценивалось время работы батарей радиозакладки, определялся состав группы с учетом специальных навыков сотрудников и тип требуемой техники.

Объектами оперативно-технических мероприятий могли быть лицо или телефонная линия учреждения, здание, помещение или автомобиль. Методы, используемые для работы в отношении объектов, различались в соответствии с типом искомой информации.

Если целью мероприятия было выступление, например, военного атташе во время еженедельного служебного совещания, то устройства прослушки устанавливались в конференц-зале посольства. Если атташе рассматривался как кандидат на возможную вербовку, его слабости и наклонности могли обнаружиться в ходе прослушки спальни или личного телефона.

Для проникновения в помещение, например, третьего этажа торговой миссии, с окнами, выходящими на улицу, потребовался бы совершенно другой оперативный план, чем для радиозакладки в зале заседаний генералитета внутри зоны безопасности на военной базе. При отсутствии незаметного доступа к месту расположения объекта операция прослушки становится невозможной.

Специалисты рассчитывали время безопасного пребывания внутри помещения, оптимальную дату и время установки оперативной техники, предполагаемые пути ухода с объекта, индивидуальные требования к оперативному прикрытию и риски в случае раскрытия операции. Резидентура и Центр оценивали значение информации, которая могла быть получена в результате успешной операции.

На основании собранных сведений о месте мероприятия сотрудники готовили план проникновения на объект и подготовки места для оперативной техники, включая сверление стены,

установку радиозакладки, восстановление вскрытых участков стен, «зачистка» следов работы, сбор инструментов и безопасный уход с объекта.

В план мероприятия также вносились режимы связи с группой наблюдения и последовательность действий в чрезвычайных ситуациях: что нужно делать при возникновении технических сложностей или проблем с безопасностью в ходе мероприятия.

Специалист должен был скрытно просверлить стену (пол, потолок) и замаскировать микрофонное отверстие, а также установить микрофон, проложить до нужного места. Все кабели сводились в отдельное секретное помещение, желательно без окон, которое называлось постом прослушки (далее – ПП), где устанавливались магнитофоны для записи разговоров.

После установки радиозакладка проверялась ПП. Отчет включал сведения о месте мероприятия, оборудовании и задействованных сотрудниках. Резидент нес ответственность за персонал на ПП, наличие магнитофонов, за перевод и подготовку стенограммы, в то время как техник обеспечивал прием информации и техническое обслуживание оборудования.

После окончания мероприятия оперативники организовывали второе тайное проникновение на объект для извлечения оперативной техники и восстановления места ее установки. Но эта задача не всегда была выполнимой по разным не зависящим от оперативников причинам. Поэтому было важно грамотно оценить все риски во время изъятия техники и сопоставить их с последствиями ее потери в случае невозможности забрать ее с объекта.

В процессе оперативно-технических мероприятий техника должна устанавливаться тайно – без видимых изменений интерьера комнаты. Обстановка на объекте внедрения была для оперативников величиной постоянной. И если какие-либо физические особенности объекта требовалось изменить, это должно быть сделано своевременно, чтобы затем все тщательно восстановить.

Несмотря на сложные обстоятельства, они творили «чудеса». Специальная техника в сочетании с их мастерством позволяла записывать частные беседы людей, к которым у спецслужб не было доступа. Настроения, мысли и желания потенциальных кандидатов для вербовки записывались на кассеты, что давало оперативникам возможность быть в курсе жизни потенциальных агентов.

А записи обсуждений официальных политических и дипломатических стратегий обеспечивали аналитиков спецслужб и руководство траны сведениями из достоверных источников. Кроме такой стратегической информации, были сведения и тактического назначения, помогавшие планировать и корректировать операции контрразведки.

Прослушиваемая информация по кабелю, а позднее по радиоканалу, поступала на ПП. Все факторы – особенности объекта, сотрудничество резидентуры с местными службами безопасности и расстояние до ПП – учитывались для выбора канала передачи данных – по кабелю или радиоэфиру, а сегодня с помощью лазерной или волоконно-оптической системы.

Если ПП расположен близко к объекту, например в подвале жилого дома или в соседней комнате отеля, лучше задействовать кабель, а не радиоканал. Проводные микрофоны или видеокамеры не требуют питания от электросети объекта и могут быть установлены в местах, где их невозможно обнаружить без спецтехники.

Однако проводные системы прослушки устанавливались, как правило, медленнее, а их кабели нередко случайно обнаруживались во время какого-нибудь ремонта помещений.

Для проводных прослушивающих систем разрабатывались специальные инструменты и комплекты для скрытой установки микрофонов и прокладки проводов. Эти комплекты применялись и для тайной прокладки тонких кабелей под окрашенные поверхности.

Чтобы ускорить оперативно-техническое мероприятие, техники иногда сами изготовливали портативный инструмент с острым специальным раздвоенным ножом для подрезания обоев. С его помощью можно было быстро установить в место разреза специальные тонкие проводники и затем легко восстановить прежний вид места вскрытия.

Как правило, техники прятали провода за деревянные плинтусы или под украшения на стене, где было сложно их обнаружить. Для этого изготавливалась легкая алюминиевая фомка длиной около 30 см. Ее как рычаг использовали для расширения щели между деревянными украшениями на стене или между плинтусом и стеной, чтобы засунуть тонкие провода, не повредив их и не оставляя следов на стене и плинтусе.

Для установки акустической системы в предметы из дерева и стены создавались специальные быстросохнущие замазки и краски без запаха, чтобы скрыть следы тайной работы. Если все шло по плану без проблем, монтаж завершался и все признаки шпионской работы скрывались в течение одного проникновения.

На ПП информация принималась, записывалась и первоначально оценивалась. Прослушка обычно велась специально подготовленными контролерами, оснащенными наушниками с усилителями, которые осуществляли запись на магнитофон для фиксации оперативной актуальности каких-либо деталей разговора. На ПП могло быть несколько магнитофонов, каждый из которых подключался к отдельному микрофону.

В 1960-е годы с появлением транзисторной техники стало проводиться все больше прослушивающих мероприятий и потому оперативники и «слухачи» все больше зависели от навыков друг друга. Технику прослушки начали активно устанавливать скрытно в помещениях как на территории страны, так и по всему миру.

Оперативно-техническим работникам приходилось работать быстро и в чрезвычайно напряженной обстановке, в условиях постоянной угрозы раскрытия проводимой операции. Ошибки и просчеты могли стоить дорого, поскольку вторая возможность проникновения в помещение могла и не представиться. К тому же нельзя было оставлять никаких следов пребывания посторонних в помещении.

В тех случаях, когда кабель нельзя было вывести за пределы нужного объекта, устанавливался замаскированный магнитофон, и его ленты регулярно менялись, например, завербованным работником, который имел доступ на объект. То, что нужно было спецслужбе, так это надежные радиопередатчики от места установки микрофона до поста прослушки.

Скрытый радиопередатчик не требовал кабелей, но не мог долго работать без замены батарей электропитания и, кроме того, радиосигнал мог быть обнаружен радиоконтрразведкой. Найти микрофон и кабели гораздо труднее, так как они не излучали радиосигналов, но провода требовали больше времени для установки и могли быть обнаружены лишь во время целенаправленного поиска.

Для радиопередатчиков систем прослушки наиболее важными являются следующие параметры:

1) надежность всех компонентов и источников питания;

2) возможность маскирования, которая зависит от размеров и конфигурации передатчика;

3) скрытность работы (противодействие обнаружению), зависящая от наличия прямых или косвенных радиоизлучений и свойств материалов, из которых передатчик изготовлен.

Развитие электроники сделало технику меньше, снижая ее энергопотребление и делая более надежной. Появление транзисторов оказало большое влияние и на оперативную технику. Когда появилась более современная техника, возникла потребность в подготовленных кадрах, которые должны были устанавливать новые системы по всему миру, а также грамотно их обслуживать.

Внедрение оперативной техники часто сопровождалось неожиданными обстоятельствами, когда приходилось быстро принимать решения, если техника давала сбой. Быстрый поиск неисправности ночью в каком-то подвале или попытка ремонтировать технику, имея ограниченный набор комплектующих, требовали от специалистов особых способностей.

Оперативно-техническая служба всегда нуждалось в сотруднике нового типа, который сочетал бы в себе качества быстро соображающего, целеустремленного и готового действовать «креативно», но при этом технически подготовленного «бойца невидимого фронта», склонного к приключениям.

Независимо от того, проводился ли аудиоконтроль с помощью проводного кабеля или радиопередатчика, каждая оперативно-техническая операция требовала детального планирования тайного проникновения на объект и ухода с него, а также тщательно подобранных инструментов.

Также важно было обеспечить безопасность места установки «жучка» на весь период монтажа оперативной техники, включая прокладку и маскирование кабелей, установку антенны и проверку работоспособности всей системы. На выполнение всех этапов операции требовалось длительное время, при этом часто работы велись по ночам.

Шум от работы инструментов мог привлечь внимание и привести к провалу всей операции. Также нельзя было оставлять после своей работы никаких следов, а проложенных проводов не должно было быть видно. Хозяева квартиры, которые ничего не знали, не должны были заметить постороннего пребывания в квартире.

Сверление отверстий для «жучков» стало обязательным навыком для оперативно-технических работников. Такие отверстия для микрофонов и радиозакладок сверлились вертикально от потолка вниз, или наоборот, из подвала вверх, ну и, конечно, горизонтально внутри стены.

Когда техники не могли попасть в помещение, чтобы установить радиозакладку, они сверлили смежную с этим помещением стену. Подобная операция была довольно рискованной, поскольку стена сверлилась «вслепую». Техники не знали ее толщины и не представляли, что их ждет за ней.

Кроме опасности просверлить стенку насквозь, установка микрофона таила в себе и другую проблему – шум. Электродрель считалась быстрым, но очень шумным инструментом. Ее нельзя было использовать ночью или для сверления стены, за которой кто-то мог находиться.

Ручная же дрель работала медленно и не годилась для работы с твердыми строительными материалами. Кроме того, для безопасного сверления нужно длительное время, иногда несколько дней, особенно, если планируется установка нескольких «закладок».

В типичной операции по установке микрофона техники начинали сверление отверстия размерами около 10 мм, что немного больше диаметра микрофона, и далее продолжали сверление практически до поверхности стены помещения, которое предполагалось прослушивать.

В этой части стены изготавливалось крошечное отверстие, около 1 мм, которое было трудно заметить на поверхности. Такое отверстие создавало хороший звуковой канал для уверенного контроля человеческого голоса.

Оборудуя сквозное отверстие для микрофона, техники часто не могли точно определить, как близко сверло находится от противоположной поверхности стены. Даже самые опытные техники старались действовать крайне аккуратно, руководствуясь интуицией, чтобы не просверлить стену насквозь. Если бы такое произошло, то ситуация могла развиться самым непредсказуемым образом. На полу в другой комнате могли оказаться куски штукатурки и другой строительный мусор.

Чтобы избежать излишнего шума и пролома стены, техники часто сверлили микрофонное отверстие с помощью дрели с малой скоростью. Дрель удерживалась большим и указательным пальцами, чтобы чувствовать давление сверла и сразу определить, когда сверло будет достаточно близко к поверхности, чтобы вовремя остановиться.

Развитие потребительского рынка бытовой микроэлектроники было выгодно оперативно-технической службе. Так, в 1980-е годы широко использовались наушники для плеера вместе с дешевыми карманными калькуляторами, пейджерами и электронными часами.

В результате эти изделия были приспособлены и для скрытого применения спецслужбой. Наушники, которые раньше скрывались в ухе сотрудника, теперь маскировались под обычные наушники плеера или мобильного телефона.

Печатные платы и компьютерные микросхемы обеспечивали разработкам оперативно-технической службы миниатюризацию и гибкость при создании оперативной техники. Цифровая память как общий компонент современной микроэлектроники невероятно расширила возможности хранения и записи разведданных. Шпионская техника становилась все более неотличимой от бытовой электроники даже при тщательном исследовании.

Методы тайного внедрения систем аудио– и видеоконтроля ограничивались только воображением оперативно-технических работников. Прослушивающие устройства, вмонтированные внутри подарков, преподносились дипломатам, бизнесменам и другим контролируемым особам.

Однако в подобных операциях было 2 основных недостатка – невозможность предсказать, где подарок окажется, и степень опасности, которая грозит дарителю в случае обнаружения «жучка».

В начале 1970-х годов начали создаваться безопасные системы аудиозаписи для оперативно-технических сотрудников, которым требовались голосовые заметки во время проводимых мероприятий. Были модифицированы небольшие стереомагнитофоны «Sony» путем добавления дополнительной записывающей головки.

В стандартном режиме магнитофон воспроизводил музыку с кассеты в 2-канальном стереорежиме. Когда сотрудник хотел записать оперативную информацию, он включал установленную ОТС систему скрытой записи на 3-ю дорожку, которая в обычном режиме не прослушивалась даже при использовании другого магнитофона. Лишь сотрудник знал, как включить тайную дорожку.

Существенной особенностью этих устройств являлось то, что они были безуликовыми, то есть идентичными обычной технике и практически неотличимыми от нее. Особенно оригинальный магнитофон «Pettle» разработала британская оперативно-техническая служба. Он предоставлял возможность записи звука на неиспользуемую часть пленки между стандартными дорожками.

Цифровые технологии также позволили как разновидность шпионской маскировки использовать «электронное прикрытие» оперативно-технических мероприятий. С помощью этих новых технологий создавались шпионские программы, глубоко спрятанные в «недрах» системы управления электронным устройством.

Бытовая электроника стала многофункциональной, например обычный мобильный телефон или смартфон (iPhone) является настоящей шпионской оперативной техникой, поскольку оборудован микрофоном и камерой, хранит в цифровой памяти огромное количество медиафайлов и сообщений, а также «привязан» к сети радиосвязи. Именно это стало в XXI веке новым техническим прорывом для оперативно-технических служб.

## 2.2. Прослушка ЦРУ

7 сентября 1951 году в американском разведуправлении был создан Штаб технических служб (далее – ШТС), начальником которого стал Джеймс Драм. Он содержал всего 50 сотрудников и размещался во временной лаборатории в Индиан-Хэд в штате Мэрилэнд. Рассмотрим некоторые известные факты о работе и техническом обеспечении оперативно-технической службы американской разведки и контрразведки.

Кабельные телефонные линии были самыми уязвимыми для тайной прослушки. Обычный телефонный аппарат содержал качественный угольный микрофон, встроенный в трубку, и был связан с линиями, выходящими из здания.

В начале 1950-х годов ШТС разработал 3 основных метода для прослушки телефонов, которые в дальнейшем использовал много лет.

Первым вариантом было гальваническое подсоединение к проводам линии, что давало возможность прослушивать и записывать разговоры по ним. Для аудиоконтроля требовался физический контакт с телефонными проводами или специальный индуктивный датчик съема информации, монтируемый как муфта вокруг телефонного провода.

Вторым вариантом прослушки было использование телефона с измененной схемой. Если телефонная трубка лежала на рычаге, его контакты отключали разговорную часть аппарата от линии. В 1950-е годы ШТС разработал методику «обхода» контактов рычага, что давало возможность использовать микрофон телефонной трубки для прослушки разговоров в помещении.

Чтобы изменить микрофонную цепь, требовался доступ к телефонному аппарату. Но если удавалось узнать марку и модель телефона, то, получив такой же, ШТС вносил изменения в конструкцию телефонного рычага. После этого в нужном помещении осуществлялась замена телефонного аппарата «своим» человеком из обслуживающего персонала.

В третьем варианте прослушки использовался собственный электрический ток телефона. Напряжение и ток телефонной линии вполне достаточны для электропитания прослушивающих устройств, для которых в этом случае не требуется батарея.

В конце 1950-х годов для системы прослушки был разработан специальный радиопередатчик «СРТ-1». В его основу были положены микровакуумные лампы и недавно появившиеся транзисторы. Устройство было далеко от совершенства, но тем не менее это был крупный шаг в развитии оперативной техники.

Он позволил отказаться от проводного микрофона и прокладки к нему кабеля, обеспечил передачу прослушиваемых разговоров по радио. Однако передатчик имел размер обувной коробки и потреблял много энергии. Тем не менее, «СРТ-1» дал оперативникам возможность аудиоконтроля объекта на определенном расстоянии от пункта прослушки.

Кроме того, американскому военному атташе в Москве удавалось от случая к случаю собирать сведения об объектах, «закрытых» для иностранцев. Так, 3 марта 1953 года майор Джордж Ван Лаэтан ехал по Киевскому шоссе в аэропорт Внуково, имея при себе карманный детектор излучения радиолокаторов. Сигналы при этом записывались на магнитную проволоку. Детектору удалось засечь сигналы с новой артиллерийской позиции ПВО, которую только-только строили, за 97 км до нее.

В 1960 году Штаб технических служб реорганизовали в Отдел технического обеспечения (далее – ОТО). В этом же году в Гаване – столице Кубы «попались на горячем» и были арестованы 3 специалиста отдела по прослушке. В тот период нехватка оперативной техники заставляла специалистов самим что-то придумывать и изготавливать ее своими руками.

Так, в начале 1960-х годов один техник ОТО реализовал прослушку на базе системы оповещения, которую обычно монтируют в стенах и потолках в школах, офисах и гостиницах.

За несколько часов он сделал специальный электронный переключатель, который превратил установленные в комнатах динамики в микрофоны для прослушки.

Это рацпредложение обеспечивало как безопасность операции, так и высокую техническую эффективность использования динамиков как микрофонов. В те годы, система оповещения использовалась для объявлений, сигналов пожарной тревоги, гражданской обороны и т. п. Она была штатной частью интерьера помещений и не вызывала никаких подозрений.

Но не только настенные громкоговорители предоставляли оперативно-технические возможности по их приспособлению для прослушки. Такие бытовые приборы, как телевизоры и радиоприемники тоже можно было «улучшить», чтобы их динамики стали микрофонами или просто вставить микрофон под сеточку на передней панели динамика. Радиопередатчик удобно маскировался внутри радиоприемника как составная часть его схемы и запитывался, когда приемник подключался к электросети.

Когда специалисту необходимо было установить «жучок» в помещении, куда нельзя было зайти и соответственно просверлить отверстие для звукопровода, он применял систему стетоскопа. Принцип его работы заключался в улавливании звуковых колебаний с помощью поверхности стены или пола квартиры, соседней с нужным помещением.

Конструкция такого микрофона-стетоскопа была похожа на мембрану классического граммофона без звуковой иголки. Техник мог выдолбить небольшое углубление в полу квартиры над нужным помещением, установить туда стетоскоп и зашпатлевать это место для уменьшения влияния посторонних шумов и вибраций.

В 1962 году начальником ОТО стал Сеймур Рассел, который стал чаще организовывать сложные и смелые с оперативной точки зрения операции прослушки. Однако отказы оперативной техники в этих мероприятиях иногда достигали половины общего их количества.

Проверка оперативной техники была особой задачей в первые годы деятельности ОТО. Она изготавливалась как официально, так и неофициально. Инженеры в лабораториях и частных компаниях выполняли заказы и проверяли готовую продукцию так, как они считали нужным, а затем отправляли новые устройства спецслужбам.

Как правило, оперативно-технические сотрудники резидентур получали из Вашингтона батарейки, радиопередатчики, микрофоны и магнитофоны, чтобы затем их собрать в системы прослушки для размещения в обозначенных местах по всему миру. Нередко все компоненты соединяли в единую систему только на месте установки. Однако слишком часто система оказывалась неработоспособной.

Инженеры в лабораториях должны были в своей работе ориентироваться на место проведения мероприятия, чтобы знать к какому атмосферному и температурному режиму эксплуатации готовить оперативную технику. Также надо было учитывать, что на нее может попасть краска или клей, ее могут ударить или залить водой.

Из-за частых отказов техники сотрудники резидентур все чаще пытались ее ремонтировать своими руками. Техники, которые разбирались в электронике, могли осмотреть печатные платы и понять, что можно подправить или слегка изменить. Так, один сотрудник ОТО увидел в научно-популярном журнале микросхему и сам сделал на ее основе новый радиопередатчик.

В то же время появились проблемы с применением для операций прослушки профессиональных концертных микрофонов. Отличный угольный микрофон был настолько чувствительным, что фиксировал любой звук в комнате. Однако если он долго находился внутри стены или в других сходных условиях, угольный порошок спрессовывался, уменьшая чувствительность микрофона.

Образованный в 1962 году Директорат исследований объединил космическую разведку и спутниковые программы, наряду с финансируемыми ЦРУ другими исследованиями в этом новом подразделении. Однако ОТО и его техническое обеспечение оперативных мероприятий разведки оставались под началом Директората планирования ЦРУ.

Только за последнее десятилетие ОТО расширился от 50 сотрудников в 1951 году до подразделения в несколько сотен инженеров, мастеров, ученых, психологов, художников, резчиков печатей и технических специалистов.

После 1962 года, когда в ЦРУ был создан отдельный Директорат исследований, ОТО работал исключительно для обеспечения оперативной деятельности, а также для поддержки 20% своих сотрудников, работавших на зарубежных базах ЦРУ.

За исключением специальных направлений типа СССР и Китая, эти разбросанные по всему миру техники могли прибыть в любое место для технического обеспечения оперативных офицеров ЦРУ. Если в операции требовалось установить скрытую камеру, микрофон или организовать контроль телефона, техник мог это сделать.

Если что-то не работало, техник мог это «что-то» починить. А если оборудование не работало и после ремонта, техник мог заменить его на другую подходящую систему.

Кроме того, микрофоны или радиозакладки, которые ранее использовались исключительно для прослушки, предлагались оперативникам в качестве односторонней системы связи, если агент знал, что его будут слушать через скрытый микрофон и передатчик. Такой комплекс агентурной связи стал называться «звуковым тайником».

Так, в одном западноевропейском городе техники установили микрофон в дереве прямо в парке. Чтобы связаться с куратором, агент разговаривал с «деревом». Однажды закладку установили снаружи здания, и агент мог остановиться около «оборудованного» места здания, сказать свое сообщение и продолжить прогулку. «Звуковые тайники» стали популярными, как только стали применяться.

Оперативники ценили техников ОТО за изобретательность и оперативно-технические навыки. Однако многие офицеры, не имевшие тяги к технике, не могли освоить специальные устройства. А научный прогресс 1960-х годов требовал, чтобы специальная техника и оперативные мероприятия эффективно дополняли друг друга.

Оперативники, плохо разбирающиеся в спецтехнике, не могли представить ее потенциал, в то время как офицеры-техники боялись, что технику будут неправильно использовать и опасались задействовать ее особые возможности. Пропасть между оперативными мероприятиями и специальной техникой стала причиной того, что ОТО не получил место в новом здании ЦРУ в Лэнгли, где разместились все оперативные службы.

В 1962 году был создан Директорат исследований (с 1963 года – Научно-технический директорат), благодаря которому этапы НИОКР для космических и спутниковых программ «Глобальных технологий» теперь проводились независимо от оперативной деятельности. И ОТО оставался в Оперативном директорате с единственной целью – обеспечивать резидентуры, оперативников и агентов оперативной техникой.

В 1960-е годы операции прослушки стали приоритетными для ОТО. Правительственные телефонные каналы, офисы и объекты иностранных миссий, места проживания и гостиничные номера – все это контролировалось оперативно-техническими работниками.

К концу 1960-х годов акустическое оборудование стало гораздо надежнее, чем вначале. Процедуры испытаний устраняли большинство проблем до того, как техника попадала в резидентуры. Однако некоторые условия использования все-таки влияли на качественную и полностью проверенную аппаратуру.

Так, например, после того как один офицер ОТО успешно установил радиозакладку в одном европейском городе, прием сигнала на пункте прослушки от радиопередатчика оказался неустойчивым. Техники были озадачены тем, что даже ночью, когда техника должна работать без помех, радиосигнал периодически исчезал. Поиск неисправностей не дал никаких результатов.

Только когда сотрудник ОТО стал наблюдать за улицей через окно, он заметил мотоциклистов. Очередной сбой в работе оперативной техники случился, когда по улице между пере-

датчиком в контролируемом здании и приемником на пункте прослушки проехал момтоцикл. Стало понятным, что сигнал передатчика «зашумлялся» радиопомехами от системы зажигания мотора.

В 1966 году начальником ОТО стал Сидней Готлиб. В этом же году отдел переехал в комплекс бывшей штаб-квартиры ЦРУ в Вашингтоне.

В 1969 году первые модели радиопередатчика «СРТ» были заменены на полностью транзисторные, в результате чего количество операций прослушки увеличилось, и оперативно-техническая служба стала накапливать опыт их проведения.

Так, одна из проводимых операций стала серьезным уроком, связанным с химическими и строительными технологиями. Планировалось внедрение техники прослушки на этапе строительства посольства одной страны социалистического лагеря. С самого начала и до конца операция проходила без проблем.

Оперативник разведки завербовал строителей, которые установили более десятка «закладок» в незастывший бетон в указанных местах по всему зданию. Устройства перед установкой были проверены, и все были уверены в успехе операции. Но когда строительство посольства завершилось, и система прослушки была включена, ни одна «закладка» не работала.

После долгих размышлений и исследований эксперты пришли к выводу, что при высыхании бетон очень сильно нагрелся. Причиной этого являлись химические процессы, возникающие при взаимодействии цемента с водой. Как «побочный эффект» от таких реакций и выделяется тепло.

Однако установленные устройства в то время не могли противостоять высокой температуре. После этой истории корпуса прослушивающих устройств стали предметом пристального внимания ОТО. Теперь при планировании операции обязательно учитывались такие климатические условия, как высокая температура и влажность.

Нехватка малогабаритных и энергоемких батарей ограничивала оперативные возможности передатчиков. Если радиозакладка может функционировать всего несколько дней, то операция прослушки теряет смысл, поскольку замена батарей требовала значительных затрат и рисков, связанных с раскрытием операции.

Тем не менее сотрудники ОТО придумали, как справиться с недолговечноой и нестабильной работой аккумуляторных батарей. Они оценивали все доступное пространство, которое обеспечит установку радиозакладки с максимальным количеством батарей. Их параллельное соединение значительно увеличивало длительность работы техники.

В 1970-х годах оперативно-техническая работа американской разведки еще более активизировалась. Техническая революция заставила ОТО внедрять в оперативную технику новые интегральные микросхемы, созданные современной промышленностью.

Появление миниатюрных компонентов нового поколения, способных передавать сигналы на большие расстояния и длительное времея, привело к разработке новых маленьких по размеру радиозакладок. Установка такой техники прослушки в стены и другие места теперь называлась «пассивным оперативным маскированием».

Микроэлектроника открыла большие перспективы в методах установки систем аудио– и видеоконтроля в такие портативные устройства, с которыми было удобно работать. Оперативная техника была уже достаточно миниатюрной для того, чтобы внедрять ее в электронные бытовые устройства – зажигалки, часы, калькуляторы или радиоприемники.

Опытные техники ОТО теперь могли создавать безуликовую маскировку для оперативной техники индивидуальной прослушки. Часы и зажигалки стали первыми образцами в области «активной маскировки». При такой «крыше» можно было осуществлять аудиоконтроль практически любого человека и в любом месте.

Устройства прослушки устанавливались внутрь мебели, книги, одежды и тюбика для крема, а однажды – в строительную каску одного рабочего. Горничные в отелях или «простые»

посетители могли занести и оставить «закладку» в любом помещении, например, вручив кому-нибудь подарок или незаметно заменив настольную пепельницу на подготовленный дубликат.

Для быстрой установки комплекса оперативной техники прослушки стал применяться деревянный блок. Из радиопрозрачного дерева можно было сделать блоки любой конфигурации с помощью обычных инструментов и затем разместить их в нужном месте. Маленькие блоки делались так, чтобы не отличаться от интерьера помещения и сливаться с мебелью, украшениями или рамой картины.

Вскоре ОТО создал сверхминиатюрные микрофоны высокой надежности, которые могли противостоять механическому влиянию и нагреву. Их можно было устанавливать практически в любом месте независимо от физических и атмосферных условий. Они имели очень низкий показатель отказов независимо от мест установки.

Сложные для внедрения оперативной техники объекты требовали больших навыков и опыта, что в свою очередь использовалось для работы на еще более сложных объектах. Увеличение количества необычных оперативно-технических мероприятий потребовало более совершенного инструмента и оборудования для установки «жучков».

Когда техники не могли попасть в помещение, чтобы установить радиозакладку, они сверлили смежную с этим помещением стену. Подобная операция была довольно рискованной, поскольку стена сверлилась «вслепую». Техники не знали ее толщины и не представляли, что их ждет за ней.

Чтобы решить проблему измерения толщины стены ОТО разработал специальный «умный» инструмент. Его основой был счетчик Гейгера, который подсчитывал количество заряженных частиц, отраженных от стены. Миниатюрный радиоактивный источник генерировал импульсы, часть которых отражалась от стены и регистрировалась специальным приемником.

Он измерял количество импульсов, которое было пропорционально толщине стены. Более тонкая часть стены отражала меньшее количество импульсов и наоборот. ОТО сделал шаблон, по которому можно было оценить приблизительную толщину оставшейся части стены. Более сложная версия этого прибора позже применялась службами безопасности аэропортов для контроля багажа и людей.

В 1970-х годах инженеры ОТО разработали измерительный прибор, который устанавливался напротив микрофонного отверстия в стене. Просверлив стену на определенную глубину, техник останавливался и производил измерение оставшейся толщины стены. И так продолжалось до того момента, пока ее толщина не становилась минимально возможной.

Со временем оперативно-технический персонал настолько освоил новый вид измерений, что определял глубину сверления по щелчкам прибора. Чем медленнее происходили щелчки, тем тоньше была стена. Такие тренировки проводились и в темноте, чтобы быть готовым работать в помещении без освещения.

Кроме того, была еще одна проблема при создании микрофонного отверстия. Дело было в том, что вращение сверла приводило к выбросу мелких частиц кирпича и штукатурки через отверстие в контролируемую комнату. Получалось, что после создания отверстия в соседнем помещении все покроется слоем строительной пыли, что будет замечено сотрудниками офиса или жильцами квартиры.

Проблема пыли во время мероприятия была решена путем создания более миниатюрного отверстия в слое штукатурки. Для этого инженеры ОТО создали новое устройство, которое осуществляло сверление сжатым воздухом с высокой скоростью струи. Вся установка с принадлежностями была помещена в стандартном кейсе.

Тем временем системы прослушки совершенствовались, число типов радиопередатчиков, источников электропитания, микрофонов и монтажных инструментов увеличивалось, и техникам уже потребовалось дополнительное обучение для сборки, настройки и проверки

нового оборудования. Освоение техники прослушки теперь проходило в условиях строгого следования инструкциям.

Когда в 1964 году началась война во Вьетнаме, техники ОТО прослушивали разговоры военных Северного Вьетнама там, где был доступ к проводным линиям связи или радиоканалам. В одном из таких мероприятий информация, полученная с кабеля связи, вначале записывалась, а потом передавалась через систему секретных ретрансляторов в Лаосе на контрольный пункт в Таиланде.

По сути, эта система функционировала как сеть мобильной связи, в которых телефонный сигнал от одной вышки передавался на другую и так далее до конечного места прослушки. Самой большой проблемой при этом была не передача сообщений, а поиск мест для скрытой установки ретрансляторов.

Оборудование этой системы прослушки устанавливалось и маскировалось в деревянных столбах воздушной телефонной связи. Сложным оперативно-техническим мероприятием было перемещение по вражеской территории деревянной опоры столба со спрятанными внутри радиопередатчиком и батареями.

Эту работу доверяли завербованным вьетнамцам, которые добиралась до места, поднимались на телефонный столб, заменяли деревянный брусок на оборудованный ОТО и подключались к линии. Если операция проходила без проблем, то через ретрансляторы сразу поступали разведданные о войсках Северного Вьетнама.

Использование радиосвязи и «перехват» с линий коммуникаций было наиболее значительным вкладом ОТО в оперативные мероприятия американской разведки во время вьетнамского и лаосского конфликтов.

4 мая 1973 года ОТО был реорганизован в Управление технической службы (далее – УТС) и переведен из Оперативного директората в Научно-технический директорат ЦРУ. Начальником Управления стал Джон Макмагон. Созданием и установкой техники прослушки телефонных разговоров и оборудования для аудио– и видеоконтроля занимался 2-й отдел УТС.

После завершения конфликта во Вьетнаме, американская разведка и УТС переключились на работу с антитеррористическими программами в Европе и странах Ближнего Востока. Основным оперативно-техническим мероприятием стало внедрение специальной техники для аудио– и видеоконтроля лиц, подозреваемых в терроризме.

Эта стратегия себя оправдала, особенно, в западноевропейских странах, где члены террористических групп считали свои квартиры полностью защищенными от постороннего вторжения. Американцы полагали, что такие операции не только помогали странам предотвращать террористические акты, но и позволили укрепить и расширить сотрудничество с местными органами безопасности.

В конце 1980-х годов УТС создал направление, занимавшееся техническими исследованиями в области применения советской и другой оперативной техники, применяемой против американских объектов. Эти устройства, как правило, оказывались в УТС в результате поисковых мероприятий или приобретались благодаря связям с дружественными спецслужбами.

Инженеры, как правило, анализировали каждое получаемое устройство, чтобы определить страну происхождения, назначение, материалы, конструкцию и возможности. Это была непростая задача, поскольку разведка постоянно старалась скрыть производителя оперативной техники.

В конце концов УТС создал подразделение, которое специализировалась на переделке «добытой» техники – ее разборке и последующем создании действующего образца, оценке ее потенциала и технических возможностей. На «конвейер» поступало более 10 штук в год, и в процессе анализа надо было определить новое это устройство или старое, но модернизированное.

В 1980-е годы СССР был по-прежнему главной целью американской разведки и УТС. Анализ советской оперативной техники позволял получать важные контрразведывательные данные для ФБР, Госдепартамента и служб безопасности США.

Используя результаты анализа, инженеры восстанавливали импортную технику, тестировали и оценивали работоспособность и возможность ее применения как оперативной техники ОТО. После позитивной оценки она отправлялась в оперативные подразделения разведки для дальнейшей эксплуатации.

Оперативная техника прослушки сыграла решающую роль в освобождении 71 заложника, которых удерживали в течение 4-х месяцев боевики перуанского Революционного движения имени Тупака Амару в апреле 1997 года. 15 вооруженных террористов штурмом захватили резиденцию японского посла в Лиме во время дипломатического приема 17 декабря 1996 года.

Несколько дней спустя, когда стало очевидно, что заложников будут удерживать длительное время, спецслужбы Перу организовали оперативно-технические мероприятия прослушки в надежде получить информацию о намерениях террористов и положении заложников. Уже в январе один из заложников, чиновник перуанского правительства, вдруг попросил его изолировать от других людей.

Он начал говорить несвязно, и террористы решили, что он «сошел с ума». Однако это была хитрость чиновника, который знал о о прослушке и предполагал, что где-то находится микрофон. В течение 3-х месяцев, до 22 апреля, он сообщал через радиозакладку в иконе о положении заложников и поведении террористов.

А за минуту до штурма резиденции командой спецназа он сказал, что заложники находятся в относительно безопасных местах, а террористы на открытой местности играли в футбол. В результате проведенного штурма 15 «революционеров» были убиты, а заложники спасены, кроме одного убитого.

В 1995 году из книги «Мир шпионов» Майкла Фроста, бывшего сотрудника канадского центра связи по обеспечению безопасности, стал известен факт сотрудничества союзных спецслужб. Он рассказал, что когда советские «глушилки» в 1987 году вывели из строя аппаратуру радиоперехвата в посольствах США и Великобритании телефонных разговоров в Москве, то канадское посольство взяло на себя функции основного центра прослушки в СССР.

# Конец ознакомительного фрагмента.