Вадим Гребенников

Радиоразведка Америки

Перехват информации

Вадим Гребенников

Радиоразведка Америки. Перехват информации

«Издательские решения»

Гребенников В.

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

ISBN 978-5-44-935745-8

Радиоразведка появилась вместе с радиосвязью в начале XX века, а компьютерная разведка — вместе с глобальной сетью Интернет в 1980-х годах. Книга рассказывает историю рождения и эволюции техники и методов американской радиоэлектронной разведки и контрразведки; разработки и создания системы глобального контроля «Эшелон» и программного обеспечения компьютерной разведки США; описывает успехи радиоразведки страны по перехвату информации.«Кто владеет информацией, тот владеет миром» (Натан Ротшильд)

ISBN 978-5-44-935745-8

Содержание

Радиоразведка Америки
Перехват информации

Вадим Гребенников

Редактор Вадим Гребенников
Дизайнер обложки Вадим Гребенников

ISBN 978-5-4493-5745-8
Создано в интеллектуальной издательской системе Ridero

Предисловие

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

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

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

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

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

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

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

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

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

Этот вид разведки обладает следующими особенностями:

– действует без непосредственного контакта с объектами разведки,

– охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот,

– функционирует непрерывно в разное время года и суток и при любой погоде,

– обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации)

– добывает большое количество информации различного характера и содержания,

– получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени,

– малоуязвима и во многих случаях недосягаема для противника,

– действует скрытно, поскольку противник, как правило, не в состоянии установить факт разведки.

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

– установить несущую частоту передающих радиосредств;

– определить координаты источников излучения;

– измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);

– установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);

– определить структуру боковых лепестков излучения радиоволн;

– измерить поляризацию радиоволн;

– установить скорость сканирования антенн и метод обзора пространства РЛС;

– проанализировать и записать информацию.

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

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

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

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

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

– открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи,

– тактико-технические данные и особенности разведываемых активных радиоэлектронных средств и систем (далее – РЭС), состовляющие их «электронный почерк»,

– типы РЭС: радиосвязи, радиолокации, радионавигации, различные телеметрические системы передачи данных,

– количество обнаруживаемых РЭС противника,

– местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

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

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

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

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

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

Особенности РЭР заключаются в следующем:

– действует без непосредственного контакта с объектами разведки;

– охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот;

– функционирует непрерывно в разное время года и суток и при любой погоде;

– обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации);

– добывает большое количество информации различного характера и содержания;

– получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени;

– малоуязвима и во многих случаях недосягаема для противника;

– действует скрытно (противник, как правило, не в состоянии установить факт разведки).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Военная радиоразведка

Наряду с русской, английской, французской, немецкой и австро-венгерской армиями радиоразведка в годы Первой Мировой войны велась и подразделениями экспедиционного корпуса американских войск в Европе.

Посты прослушивания, в состав которых входили подготовленные военнослужащие, владевшие немецким языком, размещались в непосредственной близости от районов расположения немецких войск. Подключив телефонные аппараты к проводным линиям связи противника, они осуществляли прослушивание и запись передаваемых по ним телеграфных и телефонных сообщений.

Посты радиоперехвата, расположенные, как правило, на значительном удалении от линии фронта, позволяли без непосредственного столкновения с противником добывать ценные сведения о его группировке, действиях и намерениях. Возможности американской радиоразведки существенно повышались благодаря использованию постов радиопеленгации, которые определяли места расположения военных радиостанций противника.

Зашифрованные сообщения противника с постов прослушивания и радиоперехвата поступали в отдел военной разведки экспедиционного корпуса, где специалисты по дешифровке пытались раскрыть коды и шифры, которыми пользовались немецкие военные. Криптоаналитической работой в отделе в основном занимались выпускники и бывшие преподаватели армейской криптологической школы, мобилизованные на военную службу после вступления США в войну с Германией.

10 мая 1929 года в связи с закрытием «Американского Черного Кабинета» Герберта Ярдли «MI-8» Военный департамент решил объединить все армейские службы шифрования, перехвата и дешифровки в рамках войск связи. В результате ответственность за эту деятельность в Армии США была возложена на Начальника войск связи.

Чтобы лучше исполнять эти новые обязанности, Секция кода и шифра «CCS» (англ. Code and Cipher Section) в апреле 1930 года была реорганизована в службу радиоразведки «SIS» (англ. Signals Intelligence Service), руководителем которой стал Уильям Фридман.

Перед новой службой были поставлены задачи по разработке армейских кодов и шифров, перехвату сообщений, передаваемых по проводным и радиолиниям связи, пеленгации радиостанций, криптоанализа кодов и шифров противника. Часть указанных функций предусматривалось выполнять только в случае ведения армией боевых действий.

Собственную службу радиоразведки и дешифровки имел и ВМФ США, которая называлась Секцией кода и связи «Op-58» (англ. Code and Signal Section) и с октября 1917 года находилась в составе Управления военно-морских операций (англ. Office of the Chief of Naval Operations). С января 1920 года эта секция под кодовым названием «Op-18» была подчинена Начальнику связи ВМФ (англ. Director of Naval Communications).

1 июля 1922 года она под кодовым названием «Op-20-G» вошла в состав 20-го отдела Управления связи ВМФ (англ. 20th Division of the Office of Naval Communications, G Section). С января 1924 года «Op-20-G» возглавил лейтенант Лоуренс Саффорд, ставший в дальнейшем главным криптологом ВМФ США.

11 марта 1935 года на «Op-20-G» были возложены все вопросы криптозащиты военно-морских сетей и систем связи, поэтому она была реорганизована в Группу безопасности связи (англ. Communications Security Group). С марта по октябрь 1939 года и с февраля по октябрь 1942 года «Op-20-G» работала под названием «Секция радиоразведки» (англ. Radio Intelligence Section), а с октября 1939 года по февраль 1942 года – под названием «Секция безопасности связи» (англ. Communications Security Section).

В 1930-е годы в Америке нелегальное получение разведывательной информации было очень нелёгкой задачей. Раздел 605 федерального закона о коммуникациях 1934 года (англ. The Communications Act of 1934) запрещал прослушку, а также перехват переписки между иностранными государствами и США.

Начальник штаба Армии на протяжении 1937—39 годов строго выполнял инструкции и препятствовал попыткам перехвата японских дипломатических посланий, поступающих в США. Однако для генерала Джорджа Маршала, который его заменил, требования национальной безопасности были более важными.

В связи с этим воинские подразделения радиоразведки появились в США только в 1938 году – именно тогда была создана Первая рота в Форт-Монмаут, а также образованы отдельные подразделения при 5 ротах связи, расположенных в Панаме, на Гавайских островах, Филиппинах, в штате Техас и районе Сан-Франциско. В 1939 году с целью совершенствования управления созданными подразделениями на их базе в Форт-Монмаут была сформирована Вторая рота радиоразведки в составе 101-го военнослужащего рядового состава и 1-го офицера – командира роты.

Перед началом Второй Мировой войны рота имела в своём распоряжении 6 постов радиоперехвата: №1 – Форт-Хэнкок, штат Нью-Джерси; №2 – Сан-Франциско; №3 – Форт-Шафтер, Гавайские острова; №6 – Форт-Милс, Манила, Филиппины; №7 – Форт-Хант, штат Вирджиния; №9 – Рио-де-Жанейро. Перехваченные шифртелеграммы направлялись для их криптоанализа в «SIS», специалисты которой работали в здании Военного департамента в Вашингтоне.

Сначала доставка материалов радиоперехвата в Вашингтон осуществлялась авиапочтой или морем, поэтому часто в связи с плохими погодными условиями происходили значительные задержки в отправке материалов. Для исправления ситуации перехваченные и предварительно зашифрованные американским военным шифром сообщения начали передаваться в столицу по каналам радиосвязи.

Поток сообщений японского МИД, перехватываемых подразделениями армейской и флотской радиоразведок, был достаточно большим. Осенью 1941 года он составлял от 50 до 75 радиограмм в сутки, при этом объём отдельных сообщений достигал 15 страниц печатного текста. В связи с большой загрузкой специалистов по дешифровке и с целью упорядочения их работы командованием Армии и ВМФ США было принято решение, в соответствие с которым дешифровка сообщений, принятых по парным дням месяца, осуществлялась криптоаналитиками Армии, а по непарным дням – криптоаналитиками ВМФ.

Работа подразделений радиоперехвата и криптоанализа в канун вступления США в войну с Японией была достаточно напряжённой. Из 227 сообщений по вопросам японо-американских отношений, которыми обменялись МИД Японии и его посольство в Вашингтоне в период с марта по декабрь 1941 года, американской радиоразведке удалось перехватить 223 сообщения и лишь 4 радиограммы были пропущены.

К началу Второй Мировой войны «SIS» насчитывала всего 7 сотрудников. Несмотря на свою немногочисленность, в 1930-х годах ей удалось выполнить большой объём работ в области совершенствования армейских кодов и шифров, подготовки специалистов и создания новой аппаратуры шифрования и радиоразведки.

В августе 1934 года ей были переданы функции изготовления и рассылки кодовых книг и шифрдокументов, в результате чего все вопросы, связанные с криптозащитой сообщений, оказались в ведении Управления начальника войск связи Армии США.

В марте 1941 года в связи с отставкой Фридмана начальником «SIS» был назначен подполковник Рэкс Минклер. А Фридман стал у Минклера гражданским заместителем и главным техническим консультантом. Нападение Японии 7 декабря на Пёрл-Харбор стало причиной для вступления США во Вторую Мировую войну.

По состоянию на 7 декабря «SIS» насчитывала уже 181 человек (офицеров, рядовых и гражданского персонала) в Вашингтоне и 150 человек – на станциях радиоперехвата. «SIS» включала в себя Школу разведки связи, в которой учили радиоразведке и криптологии кадровых офицеров и резервистов, Вторую роту связи, которая обеспечивала штат станций радиоперехвата, и вашингтонские подразделения самой службы.

Официальная военная цензура в США была введена в декабре 1940 года, когда все коммуникации были переданы правительству для контроля. С этого момента военным подразделениям радиоразведок: армейской «SIS» и флотской «Op-20-G» было дано «добро» на осуществление программ перехвата и дешифровки.

Все материалы, которые были получены этими подразделениями, были строго засекречены и получили кодовое название «Магия» (англ. magic). Исключительная секретность, которая окружала их деятельность, позволяла избегать разоблачения.

Они сконцентрировали своё внимание на радиограммах, поскольку компании проводной связи, осознавая значение запрета, отказывались предоставлять им иностранную корреспонденцию.

Соответственно, 95% получаемой информации были радиоперехватом. Только 5% информации приходилось на перехват проводной связи и фотокопии посланий, сохранявшихся в архивах некоторых компаний, которые сотрудничали с военными.

Для перехвата радиограмм ВМФ, в основном, полагался на сеть постов радиоконтроля на Бейнбридж-Айленде в Пагет-Саунде; Винтер-Харборе штата Мэн; Челтэнхеме штата Мэриленд; Хиейя в Оаху; Корехидоре, а также более мелкие станции на Гуаме, в Империал-Бич в Калифорнии; Амагансетти на Лонг-Айленде и Юпитере во Флориде. Каждый из них отвечал за определенные диапазоны радиочастот. Станция на Бейнбридж-Айленде, например, контролировала радиообмен японского правительства из Токио.

Передача дипломатических посланий, как правило, осуществлялась по каналам коммерческого радио с использованием латинского алфавита. Военно-морские радиограммы использовали специальный код Морзе. Моряки перехватывали их с помощью операторов, знавших японскую морзянку, и фиксировали на специальной машинке, превращавших шифр в его латинские эквиваленты.

Сначала все станции направляли послания в Вашингтон авиапочтой. Но это происходило слишком медленно. Авиалайнер, который доставлял армейские перехваты с Гаваев на континент, в среднем летал один раз в неделю, а погода иногда приводила к отмене рейса, вынуждая посылать перехват морским путём. Буквально за неделю до Пёрл-Харбора два армейских перехвата из Рио не могли добраться в Вашингтон в течение одиннадцати дней.

Подобные задержки заставили флот установить в 1941 году радиотелетайпную связь между Вашингтоном и станциями на территории США. Станция набивала пачку перехватов на телетайпную ленту, соединялась с Вашингтоном с помощью телетайпной связи и автоматически отправляла все послания со скоростью 60 слов в минуту, втрое снижая расходы по сравнению с ручной передачей каждого послания отдельно. Армия установила телетайпную связь со своими континентальными постами только с 7 декабря 1941 года.

Армейские и морские станции перехватывали японские послания, зашифровывали их по американской системе и передавали по радио в Вашингтон. Зашифрование осуществлялось для того, чтобы японцы не узнали о криптоаналитической деятельности американцев. К этой достаточно дорогой системе радиоретрансляции было подключено только три наиболее значительных японских системы – «пурпурная», «красная» (её предшественница, которая сохранялась в отдалённых миссиях, например, во Владивостоке) и некоторые другие.

Поток сообщений японского МИД, перехватываемые «SIS» и «Op-20-G», был достаточно большим. Осенью 1941 года количество перехватов составляли от 50 до 75 радиограмм в сутки, при этом объём отдельных сообщений достигал 15 страниц печатного текста. Крип-

тослужбы были вынуждены постоянно ускорять скорость своей работы. Так, в 1939 году им было нужно три недели для того, чтобы все перехваты прошли весь путь до Госдепартамента. А в конце 1941 года этот процесс занимал уже не более четырёх часов.

Служба радиоперехвата работала чётко. Из 227 сообщений, которые относились к японско-американским переговорам и пересылались между Вашингтоном и Токио с марта по декабрь 1941 года, не было перехвачено только четыре. Вашингтон был просто завален перехватами, которые накапливались в секретной папке под названием «Magic». Крошечный аппарат криптологов физически не мог справиться с таким потоком.

Проблема была решена двумя способами. Во-первых, было сокращено дублирование в работе. Сначала обе службы «SIS» и «Op-20-G» самостоятельно расшифровывали все японские перехваты. Однако в 1940 году между ними была достигнута договорённость о распределении обязанностей: сообщениями из Токио по непарным дням занималась «Op-20-G», а по парным дням – «SIS». Тем самым экономилось время для раскрытия нерасшифрованных систем и ликвидации завалов. Другим способом стало раскрытие, в первую очередь, наиболее важных сообщений; другие сообщения приходилось откладывать, по крайней мере, до окончания работы над более важным материалом. Считалось, что более важные сообщения «закрывались» более сложной системой кодирования.

6 декабря 1941 года криптослужбы США получили перехваченную зашифрованную японскую телеграмму в Вашингтонское посольство и в тот же день её расшифровали. Она состояла из 14 частей, но важнейшая последняя часть, где говорилось о разрыве переговоров Японии и США, была передана из Токио лишь ночью с 6 на 7 декабря. Благодаря напряжённой работе криптоаналитиков 14-я часть была расшифрована уже в восемь часов утра 7 декабря и отправлена Президенту США. Интересно, что в японском посольстве последняя часть была расшифрована лишь в тринадцать часов, то есть американское правительство прочитало японскую ноту в полном объёме на несколько часов раньше японского посольства в Вашингтоне.

К сожалению, огромный и кропотливый труд американских криптослужб не смог предупредить нападение Японии на военно-морскую базу в Пёрл-Харборе, который произошло в тринадцать часов (по Вашингтонскому времени) 7 декабря 1941 года. Во-первых, несмотря на большой объём дешифрованной японской переписки, ни в одной телеграмме не шла речь о нападении на Пёрл-Харбор. Во-вторых, американская военно-морская разведка не имела никакой информации о местонахождении и движении японского флота из-за его радиомолчания и других мер по безопасности связи.

Кстати, на территории базы работало подразделение радиоразведки, которое обслуживало Тихоокеанский флот США и состояло из 30 офицеров и рядовых. Его начальником был Джозеф Рошфор, перед которым стояла задача перехвата и прочтения японских радиограмм, зашифрованных военно-морским кодом «JN-25» (англ. Japanese Navy code №25).

После нападения японцев на Филиппинские острова генералу Дугласу Маккартуру было приказано покинуть Филиппины и создать базу для Армии США в Австралии. Он, понимая необходимость службы радиоразведки, своим приказом 15 апреля 1942 года создал Центральное бюро радиоразведки в Мельбурне (впоследствии оно было перебазировано в Брисбен).

В июле 1942 года капитан «SIS» Абрахам Синков прибыл в Мельбурн как руководитель американского подразделения Центрального бюро. Его формально возглавлял генерал С. Эйкин, но в действительности он редко появлялся в этой организации, поэтому фактически руководство бюро осуществлял Синков.

Он проявил хорошие организаторские способности и сумел в короткий срок сформировать единую профессиональную команду из американцев и австралийцев. Деятельность бюро радиоразведки способствовала успеху действий американской армии в воздушной войне против японцев и позволила одержать ряд побед в операциях на Новой Гвинее и Филиппинах.

После начала войны объём работы «SIS» стремительно возрос. Численность службы за предыдущие 2 года увеличилась в 9 раз и продолжала расти, в связи с чем в августе 1942 года личный состав службы перебрался из Вашингтона в Арлингтон-Холл – просторное здание прежней частной школы, расположенной в одном из предместьев штата Вирджиния на побережье реки Потомак. Практически одновременно с переездом состоялись организационные изменения в Управлении начальника войск связи Армии США.

«SIS» была реорганизована в Направление безопасности связи «SSB» (англ. Signal Security Branch). В её состав вошли батальон радиоразведки, школа радиоразведки и криптологии и 4 секции, имевшие литерные обозначения: «A» – административная, «B» – радиоразведки и криптоанализа, «C» – безопасности связи и криптографии, «D» – тайнописи. С целью координации деятельности полевых постов радиоперехвата в составе «SSB» была сформирована секция «E», а в декабре 1942 году – секция «F», основным назначением которой стала организация работ по созданию новой шифровальной аппаратуры для Армии США.

Основными «поставщиками» материалов радиоперехвата для криптоаналитиков Арлингтон-Холла были подразделения Второго батальона радиоразведки, созданного 2 апреля 1942 года в результате увеличения численности и изменения структуры Второй роты. При участии личного состава батальона в сентябре того же года был создан новый стационарный пост радиоперехвата в Винт Хилл Фармс (штат Вирджиния), а немного позже – еще 2 поста, в штате Калифорния и на Аляске. В период Второй Мировой войны численность батальона существенно возросла и одно время достигала около 5 тысяч человек.

В 1942 году военно-морская радиоразведка «Op-20-G» была реорганизована, на базе которой была создана Организация разведки коммуникаций ВМФ «CIO» (англ. Communications Intelligence Organization) под руководством капитана 3-го ранга Саффорда, ставшая центром спецслужб ВМФ.

Она должна была разрабатывать военно-морские шифры, перехватывать проводные и радиосообщения, пеленговать радиостанции и осуществлять криптоанализ шифров противника. Часть отмеченных функций предусматривалось выполнять только в случае ведения армией боевых действий.

Деятельность «CIO» распределялась между подразделениями в Вашингтоне, на Гавайях и Филиппинах. Филиппинское подразделение размещалось в тоннеле крепости Корехидор и было оснащено 26 радиоприёмниками, аппаратурой для перехвата передачи данных и автоматического производства схем и таблиц. Из 700 офицеров и рядовых военно-морских учреждений радиоразведки 2 трети были заняты перехватом сообщений и только одна треть – криптоанализом и переводами.

Саффорд распределил свой персонал таким образом: в Пёрл-Харборе служили наилучшие офицеры, большинство из которых имели по четыре-пять лет опыта радиоразведки; команда в Корехидоре имела всего 3 или 4 года опыта; в Вашингтоне отвечали за общее наблюдение и учёбу – здесь служили самые опытные со стажем более 10 лет. Но до 90% сотрудников не имели и годового опыта.

Саффорд разделил «CIO» на 3 секции. Руководитель 1-й, капитан второго ранга Джордж Уэлкер занимался радиоперехватом и пеленгацией, 2-й – Ли Парк – криптоанализом, 3-й – Крамер – переводом и рассылкой материалов. Самой первой задачей подразделений было добывание материалов для обработки его криптоаналитиками.

К середине Второй Мировой войны подразделения батальона находились на территории США, Аляски, Алеутских и Гавайских островов, а также в Австралии, Индии и Африке. Посты радиоразведки, находившиеся за рубежом, входили в состав войск связи соответствующих армейских командований. Отдельные подразделения батальона, например посты, расположенные в Беллмори (остров Лонг-Айленд) и Тарзани (штат Калифорния), использовались

только для радиоконтроля за работой армейских радиостанций на территории США и в ведение радиоразведки не входили.

В марте 1943 года «SSB» стала называться Службой безопасности связи «SSS» (англ. Signal Security Service). В июле того же года после соответствующего увеличения численности личного состава все секции были переименованы в отделы, а Служба преобразована в Агентство безопасности связи «SSA» (англ. Signal Security Agency) Армии США.

В течение всей войны наиболее численным среди подразделений Агентства был отдел «B» (радиоразведки и криптоанализа). Разведданные, подготовленные специалистами отдела на основании анализа перехваченных открытых и зашифрованных радиосообщений противника, направлялись в Управление военной разведки для их последующей оценки и использования. Высокая ценность докладываемых данных была обусловлена тем, что за годы войны американским криптоаналитикам удалось раскрыть много кодов и шифров противника: в 1942 году ими был разгадан шифр ВМФ Японии, а в 1943 – армейские японские шифры.

Завершающий этап войны ознаменовался для «SSA» новыми организационными изменениями. В начале 1944 года в результате проведённой реорганизации в нём были созданы четыре отдела: разведывательный, безопасности связи, вспомогательный, комплектования и подготовки личного состава. В декабре того же года Агентство было передано в оперативное подчинение Управлению военной разведки, при этом административное руководство Агентством осталось за Начальником войск связи Армии США.

6 сентября 1945 года, через 4 дня после окончания Второй Мировой войны, военным руководством было принято новое решение, в соответствии с которым «SSA» была полностью выведена из подчинения Начальника войск связи и с 15 сентября вместе со всеми своими подразделениями и военными учреждениями связи была реорганизована в Агентство безопасности Армии «ASA» в составе Генерального штаба МО США. Возглавил её коллега Фридмана – криптолог Фрэнк Роулет.

10 июля 1946 года все подразделения радиоразведки и связи ВМФ были объединены во 2-ю секцию 20-го отдела Управления связи ВМФ «Op-20-2», которая была названа «Коммуникационной вспомогательной деятельностью» (англ. Communications Supplementary Activities of the 20th Division of the Office of Naval Communications, Section 2).

23 июня 1948 года ВВС США также создали собственную радиоразведку – группу безопасности «AFSG» (англ. Air Force Security Group). 20 октября она была переименована в службу безопасности «AFSS» (англ. Air Force Security Service), которая должна была заниматься радиоперехватом и дешифровкой.

20 мая 1949 года военным руководством США было принято решение об объединении усилий всех военных радиоразведок и криптослужб: «ASA», «Op-20-2» и «AFSS». В результате было образовано объединённое Агентство безопасности Вооруженных Сил «AFSA» в составе Министерства обороны США, которую в 1951 году возглавил генерал Ральф Джулиан Канин. Через год, в 1952 году, когда «AFSA» была реорганизована в Агентство национальной безопасности США, он стал его первым директором и находился на этом посту до 1956 года.

2. Дирекция радиоразведки АНБ

Агентство национальной безопасности США (далее – АНБ) – англ. National Security Agency (NSA) – подразделение радиотехнической и электронной разведки Министерства обороны (далее – МО) США, входящее в состав Разведывательного сообществана правах независимого разведывательного органа. Сформировано в составе МО 4 ноября 1952 года. По числу военнослужащих и вольнонаёмных сотрудников и по размеру бюджета является крупнейшим в США разведывательным ведомством.

АНБ США отвечает за сбор и анализ информации средствами РЭР, контроля электронных коммуникационных сетей, учёта электронного трафика, решает высокоспециализированные задачи радиоразведки по получению информации из коммуникационных сетей зарубежных государств путём электронного и радиоперехвата и её дешифровки с применением компьютерной техники.

АНБ также несёт ответственность за закрытие электронных телекоммуникационных сетей государственных учреждений США от несанкционированного доступа служб РЭР других государств. Решает задачи получения информации техническим путём, отвечает за все виды РЭР, задачи защиты данных и криптографии.

АНБ – ещё более молчаливая, тайная и мрачная организация, чем ЦРУ. Официальные представители ЦРУ время от времени делают заявления для средств массовой информации, передают представителям прессы благоприятную для себя информацию. Официальные лица из Агентства не занимались этим никогда.

Таким образом, АНБ остаётся наиболее таинственной организацией среди американских спецслужб. Устав АНБ доныне засекречен. Лишь в 1984 году были преданы огласке некоторые его положения, из которых стало известно, что Агентство освобождено от всех ограничений на ведение разведки связи.

В первые годы после своего образования АНБ размещалось в разных зданиях, разбросанных по всему Вашингтону. В 1954 году Министерство обороны США заключило контракт на строительство для АНБ специального большого здания в Форт Миде (штат Мэриленд). Строительство было в основном закончено осенью в 1957 году, но только в начале следующего года новоселье справили последние сотрудники АНБ.

И хотя этот «храм» перехвата и прослушки, несомненно, стал самым грандиозным из когда-либо, построенных для его «жрецов», он оказался для них слишком малым уже через 5 лет. Поэтому в конце 1965 года к нему был пристроен еще один девятиэтажный корпус. Расширение было вызвано невидано быстрым ростом численности сотрудников АНБ.

Директор АНБ по своему статусу должен быть военнослужащим в звании трехзвёздного генерала (т.е. генерал-лейтенанта) или вице-адмирала, который раньше работал в разведке. Он подчиняется Министру обороны и представляет АНБ в Разведывательном содружестве США.

Численность персонала на объектах АНБ, включая прикомандированных военнослужащих всех видов вооруженных сил превышает 120 тысяч человек. При этом 20—24 тысячи из них работают в центральном аппарате АНБ, другие же, в основном военнослужащие, – на базах и станциях АНБ по всему миру.

Количество таких объектов, по разным данным, – сегодня свыше 4-х тысяч. Таким образом, с точки зрения численности сотрудников, АНБ, несомненно, является наибольшей среди американских спецслужб.

Бюджет АНБ, как и других спецслужб США, до сих пор засекречен. Относительно его величины существуют разные оценки. Американская «Энциклопедия шпионажа» сообщает, что «это цифра порядка 3,5 миллиардов долларов, не считая обслуживания космических спутников-шпионов».

Однако по другим оценкам, бюджет АНБ составляет около 15 миллиардов долларов. В любом случае, вопреки распространённому обману, именно АНБ, а не ЦРУ является наиболее финансируемой спецслужбой США.

Как уже было сказано, АНБ занимается технической разведкой и обработкой собранной информации, передачей полученных данных заинтересованным ведомствам для нужд внешней разведки и контрразведки, предоставлением разведывательной поддержки операциям американских вооруженных сил, а также проведением научных исследований и внедрением разработок в сфере технической разведки.

Вторая группа задач, которые возложены на АНБ, связана с выполнением контрразведывательных функций. Это обеспечение безопасности линий секретной связи, ведения внешней шифрованной переписки, разработка кодов и шифров для передачи секретной информации и специального оборудования связи.

В состав АНБ входят 2 дирекции: Дирекция радиоразведки, ответственная за получение сведений из зарубежных каналов связи и Дирекция информационной безопасности, занимающаяся защитой электронных систем связи и информации системы США.

Дирекция радиоразведки занимается радиоэлектронными и компьютерными разведывательными операциями (от перехвата до криптоанализа), анализом движения сигналов и анализом расшифрованных сообщений.

Основными элементами его организационной структуры являются следующие подразделения:

– F – Special Collection Service (SCS) – Служба специального сбора, которая была создана в 1978 году совместно с ЦРУ для организации перехвата и прослушки в труднодоступных местах, таких как посольства иностранных государств, центры связи и правительственные учреждения иностранных государств.

– S – Signals Intelligence Directorate (SID) – Директорат радиоразведки, который отвечает за сбор, анализ, обработку и распространение данных радиоразведки, состоит из следующих подразделений:

– S1 – Customer Relations (CR) – Отношения с клиентами.

– S2 – Analysis and Production Centers (APC) – Центры анализа и обработки, имеющие следующие направления:

– S2A – Южная Азия,

– S2B – Китай и Корея,

– S2C – международная безопасность,

– S2E – Ближний Восток/Азия,

– S2F – международная преступность,

– S2G – контрраспространение,

– S2H – Россия,

– S2I – борьба с терроризмом,

– S2J – оружие и космос,

– S2T – текущие угрозы.

– S3 – Data Acquisition – сбор данных Центров анализа и обработки для Специальной службы сбора:

– S31 – Cryptanalysis and Exploitation Services (CES) – Службы криптоанализа и эксплуатации.

– S32 – Computer Network Operations (CNO) – Операции в компьютерной сети. Подразделение идентифицирует, контролирует, проникает и собирает разведывательные данные о компьютерных системах, используемых иностранными субъектами в США.

– S33 – Global Access Operations (GAO) – Операции глобального доступа. Подразделение отвечает за перехват со спутников и других международных платформ радиоразведки. Обес-

печивает функционирование системы обработки и визуализации больших массивов данных, используемой как инструмента анализа мероприятий по сбору данных в глобальном масштабе.

– S35 – Special Source Operations (SSO) – Операции специального источника. Подразделение отвечает за все программы, нацеленные на сбор данных от крупных волоконно-оптических кабелей и коммутаторов, как внутри нас, так и за рубежом, а также через корпоративные партнерства.

С 1952 по 1975 год АНБ и его предшественники осуществляло проект «Шамрок» (англ. Shamrock – трилистник), которая заключалась в ежедневном копировании всех входящих и исходящих международных телеграмм, пересылаемых по каналам связи крупных коммерческих телекоммуникационных компаний США, и хранении их в виде микрофильмов.

Одновременно с целью ограничения распространения информации о том, что АНБ занимается перехватом и обработкой электронной информации конфиденциального характера, с 1969 по 1973 годы в США осуществлялся комплекс мер по проекту «Минарет» (англ. Minaret – исламская башня).

В 1978 году с целью обеспечения надзора за деятельностью АНБ со стороны американских правоохранительных органов в США был введён в действие Закон о контроле за сбором разведывательной информации о заграничных странах (англ. Foreign Intelligence Surveillance Act).

Для его выполнения были созданы Судебная инстанция (англ. Foreign Intelligence Surveillance Court) и Апелляционная судебная инстанция по контролю за сбором разведывательной информации о зарубежных странах (англ. Foreign Intelligence Surveillance Appeals Court).

В 1962 году ЦРУ решило не отставать от АНБ в области радиоразведки и в Научно-техническом директорате создало Управление радиоперехвата. На него были возложены разработка, эксплуатация и обслуживание новейшей аппаратуры радиоперехвата, необходимой для выполнения с максимальной эффективностью задач по сбору и анализу полученной информации, а именно:

– исследование, разработка, тестирование и производство оборудования радиоперехвата для всех операций ЦРУ,

– техническая эксплуатация и обслуживание развернутых сторонних систем радиоразведки,

– обучение агентов обслуживанию устройств радиоперехвата,

– техническая поддержка сторонних соглашений,

– сбор и анализ собранных ЦРУ данных радиоперехвата,

– поддержка радиоперехвата при агентурном проникновения согласно национальной разведывательной программы США.

В 1990-х годах АНБ озаботилось поисками оператора телекоммуникаций, который связал бы штаб-квартиру АНБ со основными станциями радиоперехвата на территории США. Поскольку по каналам связи должна была передаваться секретная информация, необходимо было, чтобы они обладали необходимой степенью защищенности и были физически отделены от каналов других сетей связи.

28 мая 1998 года АНБ провело конкурс на выполнение работ по контракту на сумму в 430 миллионов долларов сроком 10 лет. Контракт предусматривал разработку и создание защищенной телекоммуникационной сети для АНБ.

Конкурс выиграла компания «Quest». В том же году АНБ доверило ей построение аналогичной сети для подсоединения станций перехвата в Западной Европе и на Ближнем Востоке к трансатлантическому кабелю.

С 1990-х годов АНБ вело разработку системы искусственного интеллекта под условным наименованием «Сложные вопросы для разведки» (далее – СВР). Мозговую деятельность в ней

имитировали мощный поисковый движок и тысячи баз данных с различной информацией, включая сведения о звонках по телефону, отчеты об операциях по кредитным картам, общение в социальных сетях, данные из глобальных систем позиционирования, история покупок в интернет-магазинах и поисковые запросы в интернете.

Работа над системой СВР, распознавание лжи, контроль над мыслительным процессом и идентификация диктора по фрагменту его речи – все это стало частью проекта модернизации АНБ под названием «Новатор». Начало ему было положено в 2000 году по распоряжению директора АНБ Майкла Хейдена.

27 февраля 2001 года руководство компании «Quest» получило совершенно неожиданное предложение – предоставить АНБ доступ к абонентской и биллинговой базе данных компании «Квест», а затем установить на своих коммутаторах оборудование АНБ для перехвата сетевого трафика – так называемые съемники.

Юридические советники компании заявили, что предложенное АНБ сотрудничество противоречит американскому «Закону о конфиденциальности электронных сообщений», который был принят в 1986 году. Поэтому для себя Наччио решил, что если АНБ желает получить доступ к сообщениям, проходящим через коммутаторы его компании, пусть приходят с разрешением судебной комиссии по надзору за внешней разведкой.

В начале 2001 года президент компании «Quest» Йосиф Наччио узнал о том, что АНБ собирается на очень выгодных условиях нанять подрядчиков для модернизации и обслуживания своих внутренних телекоммуникационных сетей в рамках проекта «Новатор». Он был призван вернуть АНБ лидирующее положение в области передовых технологий связи и одновременно позволить сократить количество сотрудников безо всякого для себя ущерба.

Планировалось, что в рамках проекта «Новатор» сотни сотрудников АНБ, которые трудились на ниве информационных технологий, должны были перейти на работу в компании, связанные договорами подряда с АНБ. Там они делали бы все то, что и прежде, но получали бы зарплату не в АНБ, а от своего нового работодателя. Считалось, что это позволит оставшимся сотрудникам сосредоточиться на решении на профильных для АНБ задач – перехват и дешифровка.

Компания «Quest» предложила АНБ свои услуги и была включена в список 35 участников операции «Новатор». Тем не менее, в апреле 2007 года сам Наччио был осужден на 6 лет тюрьмы по обвинению в инсайдерской торговле. На судебном процессе он заявил, что обвинение является ложным и инспирировано АНБ в отместку за его нежелание с ним сотрудничать. Однако при вынесении приговора суд отказался принять во внимание это обстоятельство.

Когда 11 сентября 2001 года США подверглись террористической атаке, только 7% всех зданий АНБ были расположены за пределами территории ее штаб-квартиры. Осознание того факта, что, нанеся серию ударов по довольно ограниченной площади, террористы могут фактически стереть агентство с лица земли, заставило Хейдена приступить к решению вопроса о том, чтобы переместить часть управлений и служб в другие районы США.

Другой причиной необходимости их перемещения стали проблемы с электропитанием. Дело дошло до того, что в начале 2000-х годов АНБ было вынуждено отказаться от установки двух новых суперкомпьютеров из опасения Агентства. В 2006 году, по оценкам экспертов, от подобного развития событий АНБ отделяло от 2 месяцев до 2 лет.

А мощность сети резервного электропитания была такова, что ее не хватало для удовлетворения потребности в электричестве всей штаб-квартиры АНБ. Кроме того, в АНБ эксплуатировалось большое количество высокоточного оборудования, которое было очень чувствительно по отношению к скачкам электропитания. И даже если бы оно не вышло из строя при сбое в электропитании, его все равно потребовалось бы его заново калибровать, на что потребовалось бы значительное время.

В качестве временной меры в АНБ было решено закупить дополнительные электрогенераторы и выключить старые суперкомпьютеры, разработанные во времена «холодной» войны для взлома советских шифров. Для снижения нагрузки на электросеть летом 2006 года пришлось даже отрегулировать кондиционеры так, чтобы температура в зданиях штаб-квартиры АНБ могла подниматься на 2 градуса выше установленной прежде нормы.

В августе 2005 года новым директором АНБ был назначен Кейт Александер. В связи с тем, что «Новатор» не оправдал возложенных надежд, он решил запустить новый проект «Турбулентность», который сразу же наглядно продемонстрировал, что назван так был отнюдь не зря. В одном из документов, подготовленных сенатским комитетом по делам вооруженных сил в марте 2007 года, говорилось:

«Проект модернизации АНБ „Новатор“ был завершен из-за проблем в управлении, при этом для его преемника оказались характерны те же самые недостатки в менеджменте, которыми страдает АНБ с момента окончания „холодной“ войны».

Один из сотрудников АНБ так охарактеризовал основополагающую разницу между проектами «Новатор» и ««Турбулентность»:

«Новатор» пытался объять необъятное. А «Турбулентность» стартует с небольших тестовых проектов и пытается проверить, что из них может выйти. Если тестовый проект срабатывает, то его развивают, если нет, то выбрасывают на помойку. Смысл в том, чтобы тратить деньги понемногу на проверку каких-то идей и смотреть, что из них получится.

Не получилось – забыли, получилось – переходим к следующей идее. В «Новаторе» они старались разработать целиком всю систему с нуля. Александер считает, что всеобъемлющая концепция не для него, начинать надо с малого и смотреть, что из этого выйдет и будет ли оно жизнеспособно».

В 2006 году была произведена крупномасштабная модернизация АНБ в целом. На это АНБ были выделены миллиарды долларов. В результате автоматизированные рабочие места аналитиков и переводчиков АНБ перестали представлять собой некое подобие боевых командных центров со множеством системных блоков и мониторов, опутанных хитросплетениями соединительных проводов и кабелей. Прежде из соображений безопасности обработка сведений разной степени секретности велась на отдельных компьютерах.

Например, один компьютер использовался для работы с дешифрованными египетскими дипломатическими депешами, другой – с перехватом радиопереговоров иракской военно-морской базы, а третий – для выхода в интернет. С внедрением в АНБ технологии виртуализации потребность в нескольких компьютерах отпала.

Отныне можно было иметь всего один компьютер, на котором сосуществовали сразу несколько специализированных виртуальных сред. Каждая из них была предназначена для обработки определенного типа данных, отделена от других сред и защищена паролем.

В конце концов все операторы станций перехвата АНБ были оснащены защищенными смартфонами со встроенными модулями беспроводной связи. Эти смартфоны позволяли операторам вести между собой секретные разговоры и подключаться к внутренним сетям АНБ.

В январе 2006 года Президент США Джордж Буш во время посещения штаб-квартиры АНБ заявил, что он на 100% поддерживает сверхсекретную работу сотрудников АНБ. Подчеркнув, что большинство достижений АНБ остаются тайной, Буш назвал электронную разведку, которую осуществляет Агентство, жизненно важной для США в войне с терроризмом.

При этом он опять выступил в защиту программы прослушки телефонных переговоров по всему миру, которую в рамках борьбы с терроризмом АНБ осуществляет с разрешения «Белого дома», в том числе на территории США.

Во время закрытой встречи в Капитолии сотрудники АНБ признали, что для прослушки внутренних телефонных звонков в США им требуется не решение суда, а решение аналитика.

Об этом сообщил представитель Нью-Йорка в Конгрессе от Демократической партии США Джеррольд Надлер.

В случае возникновения необходимости получения доступа к данным достаточно решения специалиста АНБ, и всё производится без правовых санкций. Вероятно, что прослушкой занимаются тысячи рядовых сотрудников, что допускается правовой интерпретацией Министерства юстиции США.

Поскольку к электронным письмам, «SMS» и сообщениям интернет-мессенджеров предъявляются те же стандарты, что и к телефонным звонкам, АНБ также имеет доступ и к текстовым сообщениям без разрешения судебных инстанций.

Бывший технический руководитель АНБ Уильям Бинни, принимавший участие в модернизации глобальной сети прослушки, заявил, что Агентство записывает и прослушивает телефонные звонки, производимые особым списком, в котором содержится от 500 тысяч до 1 миллиона сотрудников.

Благодаря закону, принятому Конгрессом США в 2008 году и продлённому в 2012 (поправки «FISA»), «AT&T» и другие компании, позволяющие АНБ контролировать их коммуникации, получают полный иммунитет от гражданской ответственности и уголовного преследования.

То, что сотрудники АНБ имеют доступ к содержимому телефонных переговоров, признавала и глава Комитета по разведке Сената США Дайэна Фейнштейн. О том, что телефонные разговоры записываются и к сделанным в прошлом звонкам внутри США можно получить доступ, упоминал Тим Клемент, бывший сотрудник ФБР.

Брюстер Кейл на основе собственного обширного опыта основателя Архива Интернета, ресурса, хранящего петабайты информации, приводит расчёты стоимости хранения всех внутренних звонков США в год в облачном хранилище в целях их обработки и анализа. Согласно его данным, для этого без учёта расходов на повышенную безопасность и разграничение доступа понадобится лишь 27 миллионов долларов в год. Для сравнения: годовой бюджет АНБ составляет около 10 миллиардов долларов.

В завершение нужно отметить, что в декабре 2014 года обе палаты Конгресса США одобрили законопроект, существенно расширяющий полномочия спецслужб по ведению электронной разведки за американскими и иностранными гражданами.

Речь идёт о поправке к закону об ассигнованиях на нужды разведки США на 2015 финансовый год. Эта поправка – так называемый «раздел 309» – разрешает сбор, хранение и распространение информации о частных телефонных переговорах и электронной переписке граждан, причём без санкции суда.

Указанная поправка впервые официально узаконивает шпионаж за гражданами США без соблюдения законных процедур. Раздел допускает, что частные коммуникации американцев, полученные спецслужбами без судебного ордера, могут передаваться внутренним правоохранительным органам для уголовных расследований, то есть спецслужбы получают практически неограниченный доступ к коммуникациям каждого американца.

Новое решение по сути законодательно закрепляет порядок сбора разведданных, установленный еще в 1981 году Указом Президента США Рональда Рейгана №12333. На его основании ничто не мешает АНБ собирать и хранить все коммуникации – не только метаданные, но и содержание. Ни ордера, ни судебного согласия не требуется, и перед Конгрессом отчитываться тоже не обязательно.

24 октября 2017 года сенатский комитет по разведке Конгресса США поддержал продление до конца 2025 года действия закона о проведении слежки за рубежом американскими спецслужбами. Закон о прослушке в интересах внешней разведки, принятый в 2008 году, позволяет сегодня разведке собирать данные об иностранцах за пределами страны. В частности,

в законе содержится так называемая «Секция 702», дающая право вести прослушку и перехват электронных коммуникаций граждан других государств.

«Черной» страницей в истории АНБ стал побег ее сотрудника Эдварда Сноудена, который с секретными файлами 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 информации.

В начале июня 2013 года Сноуден передал газетам «The Guardian» и «The Washington Post» секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за телефонными и интернет-коммуникациями во всем мире. По сообщению Пентагона, Сноуден предварительно похитил 1,7 миллиона секретных файлов, большинство из которых касается «жизненно важных операций американской армии, флота, морских пехотинцев и военно-воздушных сил».

По утверждению главы АНБ Кита Александера, Сноуден передал журналистам до 200 тысяч секретных документов. АНБ обращалось к сотрудникам министерств и ведомств США, таких как Белый дом, Госдепартамент и Пентагон с просьбой предоставить телефонные номера влиятельных политических деятелей других стран. Агентство планировало включить эти данные в свои системы слежения.

В результате один из чиновников передал АНБ около 200 номеров, среди которых оказались также 35 телефонов неназванных лидеров стран. При этом в документе, датированном октябрем 2006 года, указано, что такой сбор сведений принёс мало ценной разведывательной информации.

Согласно справке АНБ, датированной 2010 годом, сотрудники АНБ устанавливали прослушивающие «закладки» в кабинетах, которые занимали европейские чиновники в Вашингтоне и в штаб-квартире ООН, а также в Брюсселе, где располагается Совет Евросоюза. Американцы также имели доступ к электронной почте и документам европейцев.

Стало известно, что АНБ осуществляло широкомасштабное прослушивание разговоров граждан Франции, Италии и Нидерландов. Так, в период с 10 декабря 2012 года по 8 января 2013 года Агентство перехватило 70,3 миллиона телефонных разговоров и сообщений «SMS» (англ. Short Message Service – служба коротких сообщений) мобильной связи.

Ряд номеров телефонов при использовании их владельцами автоматически записывались оборудованием электронной разведки. Перехваченные «SMS» автоматически анализировались на наличие тех или иных ключевых слов, указывающих на их содержание. В электронную базу вносились данные о номерах собеседников прослушиваемых лиц, времени и длительности разговора.

Технология прослушки в АНБ обеспечивалась системами «DRTBox» и «WhiteBox». С помощью первой за указанный период во Франции было перехвачено 62,5 миллиона разговоров и писем, по второй – 7,8 миллиона. В день в среднем перехватывалось до 3 миллионов звонков и «SMS», а при пиковых показателях – до 7 млн.

Система «DRTBox» была разработана комманией «Digital Receiver Technology», входящей в корпорацию «Boeing» в Мэриленде.

«DRTBox» – военная технология контроля, позволяющая отследить и прервать тысячи вызовов сотовых телефонов, бесшумно прослушивать переговоры, перехватывать электронные письма и сообщения «SMS». Система способна одновременно прослушивать тысячи соединений мобильных телефонов, помогая отследить и записывая одновременно информацию граждан.

«DRTBox» могут оборудоваться вертолеты, самолеты, суда и подводные лодки. Принцип работы – подмена вышки сотовой связи. При этом все мобильные телефоны автоматически

соединяются с самой близкой вышкой сотовой связи, которая обладает самым мощным сигналом.

Секретная программа АНБ, работающая по Франции, носила название «US-985D». Возможно, что это обозначение «третьей группы» прослушиваемых стран, к которой относятся также Германия, Польша, Австрия и Бельгия. Во «вторую группу» входят более близкие по своей политике к США страны – Великобритания, Канада, Австралия и Новая Зеландия.

Объектами шпионажа были также Китай, Иран, Пакистан и Латинской Америки. Обнаружилось, что осуществляется массовый негласный съём огромного количества информации прямо с центральных серверов и магистральных линий связи, расположенных в разных странах по всему миру.

Многие из этих разведывательных программ дублировали друг друга и были связаны между собой в секретную информационно-коммуникационную систему. В них участвовало не только АНБ, но также Министерство юстиции и ФБР, которым это было разрешено законодательством США, например, поправками 2008 года к закону о внешней разведке (англ. FISA Amendments Act of 2008), а также судебными решениями, вынесенными Судом по делам внешней разведки США (англ. Foreign Intelligence Surveillance Court).

Кроме того, в рамках многих разведпрограмм АНБ осуществлялось сотрудничество не только спецслужб США с коллегами других стран, но и с крупнейшими частными операторами телекоммуникаций и интернет-провайдерами: «Verizon», «Telstra», «Google» и «Facebook».

«Google», например, собирает все данные пользователя, какие только есть: IP (англ. Internet Protocol address – адрес интернет-протокола) – уникальный идентификатор компьютера при подключении к интернет; ID (англ. (англ. Identifier – опознаватель) – индивидуальный номер подключения к интернет, позволяющий идентифицировать пользователя; конфигурация ПК; диагональ дисплея; версия браузера и т. п. АНБ всё нужно загрузить в свою БД на всякий случай.

В рамках операции «AuroraGold» АНБ и ШКПС мониторили около 1200 адресов электронной почты и телефонов, принадлежащих сотрудникам крупнейших сотовых операторов. Их целью было выявление уязвимых мест в технологиях мобильной телефонной связи, которые можно было бы использовать для шпионажа.

Операция «Auroragold» была нацелена на получение доступа практически к каждой мобильной сети мира. В общей сложности сотрудники спецслужб вели наблюдение за пользователями 700 мобильных сетей из 985 имеющихся сейчас в мире (около 70% всех операторов сотовой связи).

Для этого на компьютеры ключевых сотрудников «интересных» компаний было установлено вредоносное программное обеспечение. Удалённый доступ к этим системам позволил АНБ раскрыть используемое в сетях «3G» шифрование.

Если ранее предполагалось, что разведывательные ведомства могут скомпрометировать широко распространённый стандарт «A5/1», то сейчас стало известно, что в 2012 году британская ШКПС «взломали» более надёжное шифрование «A5/3».

Среди компаний, являющихся объектом слежки, упоминается «GSM Association» – крупнейшее объединение, в которое входят около 800 операторов сотовой связи и которое сотрудничает с такими компаниями, как «Microsoft», «Facebook», «Intel» и «Cisco», а также «Sony», «Nokia», «Samsung», «Ericsson» и «Vodafone».

Позже стало известно и о том, что АНБ имеет возможности для получения скрытого доступа к конфиденциальным данным пользователей многих мобильных устройств, работающих под управлением ОС «Android», «iOS» и «BlackBerry», включая местонахождение устройства, электронные записные книжки, сообщения «SMS», файлы и другие данные.

3. «Киберопасность» АНБ

Ещё с 1940-х годов АНБ годов начала «подрывать» эффективность криптосистем других стран. Наиболее важной мишенью активности АНБ стала известняя швейцарская компания «Крипто АГ» (англ. Crypto AG), созданная шведом Борисом Хагелином. «Crypto AG» имела сильные позиции как поставщик систем кодирования после Второй Мировой войны.

Много правительств тогда не доверяло оборудованию, которое предлагалось для продажи ведущими мировыми державами. Швейцарская компания в этой сфере имела лучшую репутацию благодаря имиджу нейтральности и честности Швейцарии.

АНБ добилась того, чтобы системы шифрования, использовавшиеся «Crypto AG», были скомпрометированы. Секретная операция АНБ была проведена через основателя и владельца компании Бориса Хагелина и включала периодические визиты в Швейцарию «консультантов» из США, которые работали на АНБ.

Так, в августе 1957 года «отец» американской криптологии Уильям Фридман сначала посетил Великобританию. Предметом его переговоров с сотрудниками ШКПС стали шифраторы «Crypto AG» и «AB Cryptoteknik». Сразу после этого Фридман побывал в Швеции, где встретился с Борисом Хагелином.

В итоге в следующее поколение шифраторов «Crypto AG» и «AB Cryptoteknik» был намеренно внесен изъян, заключавшийся в том, что ключ, который использовался для шифрования сообщения, вставлялся в открытом виде в шифровку. Таким образом, АНБ могло знакомиться с содержанием таких шифровок одновременно с их законными получателями.

В результате американская пресса получила копии конфиденциальных документов «Crypto AG» с записями участия представителей АНБ в обсуждении разработки новых машин в 1973 году. Было обнаружено, что в течение длительного времени АНБ перехватывало и расшифровывало секретную информацию почти 120 стран, которые пользовались оборудованием «Crypto AG».

С другой стороны, АНБ проводит «шпионские» операции по сбору развединформации в интересах американского правительства. Она осуществляет перехваты данных трафика сети Интернет. Для того, чтобы все проходило без проблем, была проведена «небольшая» подготовительная работа. Агентство потратило много времени и усилий на то, чтобы заставить производителей программного обеспечения, а также коммутаторов и маршрутизаторов внести в свою продукцию необходимы изменения.

Например, программисты могут при написании исходного кода программ включить туда модули, реализующие какие-нибудь не документируемые возможности. Причём такие «шпионские вставки» очень трудно найти. Цель очень простая – гарантировать правительству США свободный доступ к чужим зашифрованным данным.

Целью АНБ было также обеспечение иллюзии надёжности систем шифрования для других шифровальщиков, в то время как для них самих процесс дешифровки был бы простым. Каждый раз при использовании криптосистемы пользователи могли выбрать длинный цифровой ключ, который изменялся периодически. Естественно, пользователи хотели иметь свои ключи, неизвестные АНБ. Для поддержки доверия пользователей, система шифрования должна была действительно работать и быть сложной для дешифровки.

Решение АНБ состояло в разработке криптосистемы таким образом, чтобы она передавала используемый ключ получателям. Для предотвращения получения ключа несанкционированными получателями ключ пересылался в зашифрованном виде, но таким шифром, который известен только АНБ.

Таким образом, каждый раз, когда АНБ перехватывала сообщение, зашифрованное данной системой, она могла сначала прочитать зашифрованную часть сообщения, названную

«полем информационной подсказки» и выделить используемый ключ. После этого она уже могла прочитать сообщение даже быстрее, чем его санкционированный получатель.

С целью перехвата информации в сети интернет АНБ всячески стремится к тому, чтобы ослабить экспортные версии программ криптозащиты американских компаний. Такая технология была использована в 1995 году, когда появились системы криптозащиты, встроенные в программные продукты, производимые компаниями «Microsoft», «Netscape» и «Lotus» для использования в сети интернет.

Под натиском АНБ компании согласились снизить степень защиты, предоставленную пользователям за пределами США. В программе «Lotus Notes» была надёжная система электронной почты с 64-битным ключом. Это позволяло обеспечить средний уровень безопасности, который сейчас может быть раскрыт АНБ только через месяцы или годы работы.

По рекомендации АНБ компания «Lotus» вмонтировала в свою систему «скрытую отмычку», или «черный ход» (англ. black door), в результате чего Агентство получило доступ к зашифрованной электронной почте пользователей программного обеспечения «Lotus Notes».

В то время это программное обеспечение применялось для конфиденциальной переписки в правительственных заведениях Швеции, использовалось 15 тысячами сотрудниками налоговых служб и 400—500 тысячами шведскими гражданами. «Lotus Notes» включало «фактор сокращения нагрузки» во все сообщения, которые посылались неамериканскими пользователями системы.

Этот «фактор», закодированный с помощью «публичного» ключа, который мог быть прочитан только в АНБ, передавал 24 из 64 бит ключа, используемого при шифровании. Это было обнаружено шведским правительством в 1997 году и вызвало у него сильный шок.

Это стало возможным потому, что в систему защиты электронной почты «Lotus Notes», предназначенную для экспорта, был включён модуль, который давал АНБ доступ к зашифрованным данным. Это превращало задачу по раскрытию секретных сообщений в дело нескольких секунд. Компания «Lotus», которая входила в структуру компании «IBM», признала это в интервью изданию «SvenskaDDagbladet».

Аналогичные возможности были встроены во все экспортные версии веб-браузеров, созданных для пользователей сети интернет компаниями «Microsoft» и «Netscape». Каждый из них использовал стандартный 128-битный ключ для шифрования.

В экспортной версии ключ не был сокращён по длине. Вместо этого, 88 битов ключа передавалось в каждом сообщении, а 40 битов оставались секретными. Таким образом, почти каждый компьютер в большинстве стран имел встроенную стандартную возможность, позволявшую АНБ раскрыть код пользователя и прочитать его зашифрованную электронную почту.

Известный криптолог Брюс Шнайер ещё в 1999 году рассказал читателям ежемесячного электронного бюллетеня об одном таинственном сотруднике АНБ Лью Джайлзе. Он занимался исключительно тем, что вынуждал производителей ослаблять системы защиты разработанных ими программных средств. В конечном итоге, говорил он, всегда можно было все «дыры» в защите объяснить случайно допущенными ошибками.

Именно в то время в «PGP» и была введена функция «восстановления ключа», имевшая скрытый дефект, который стал недавно широко известен. Впоследствии в разных версиях этой программы были обнаружены и другие серьёзные недостатки. Например, оказалось, что в версии «PGP» для ОС «Linux» и «OpenBSD», созданных в 1997 году, генерировались слабые ключи.

Конечно, большинство обнаруженных дефектов в программах появляются, как правило, по недосмотру разработчиков. Но очень вероятно и то, что некоторые из них являются специально внедренными «чёрными ходами». В разных средствах массовой информации время от времени публикуется информация, полученная от сотрудников компаний по производству компьютерной техники и программного обеспечения, о том, как их «обрабатывало» АНБ.

Стало известно, как АНБ «вынуждало» фирмы, производившие сетевое оборудование, вносить в свою продукцию изменения в «шпионских» интересах. К компаниям, которые сотрудничали с АНБ, хотя и не всегда добровольно, относились, например, «Microsoft», «Netscape», «Sun».

Ещё в конце 1990-х годов в сети интернет появилась история о том, как один придирчивый программист, изучая исходные коды подпрограмм в ОС «Microsoft Windows NT», нашёл переменную с выразительным именем «_NSAKEY», то есть «ключ АНБ». Особого скандала из этой истории не вышло, поскольку для присутствия такой переменной нашлись более-менее невинные объяснения, а название ради общего спокойствия изменили на нейтральное «_KEY2».

Кроме того, хорошо известно, что именно АНБ, когда этого требовали американские законы, всегда контролировало снижение криптостойкости программных продуктов, предназначенных для экспортных продаж.

В начале 2005 года в сети интернет появилась статья сингапурского криптолога Хонг-Юн Ву, который исследовал конкретную реализацию алгоритма шифрования документов «Word» и «Excel» в современных версиях «Microsoft Office». Он обнаружил, что и здесь существовала достаточно серьёзная «уязвимость», которая позволяла без особых проблем раскрывать и читать файлы, защищённые шифрованием с длиной ключа до 128 бит. И причиной этому была неправильное применение потокового шифра, а именно, многоразовое использование одной и той же шифрующей последовательности.

Среди фундаментальных основ криптографии есть очень важное правило: если для засекречивания используется потоковый шифр, то никогда одну шифрпоследовательность не налагают на два разных документа. В данном контексте под «одинаковыми» документами понимаются файлы, которые совпадают байт в байт, т.е. полные копии. Любая вставка или удаление знака приводит к сдвигам других байтов на другие места, т. е. к разным файлам.

И если у «взломщика» есть хотя бы два разных документа, зашифрованного одним ключом, то всё шифрование – хотя и очень стойкое – в принципе можно раскрыть простым побитовым сложением двух шифртекстов вместе, даже не зная криптоалгоритма. При таком сложении биты шифрующей последовательности «выпадают» (взаимно уничтожаются), и остаётся сумма 2-х открытых текстов.

Имея базовые криптоаналитические навыки, а еще лучше специальные программы, «взломщик» может оба исходных документа восстановить с помощью известных криптометодов.

Как установил Хонг-Юн Ву, при реализации процесса шифрования в «Microsoft Office» была допущена именно эта криптографическая ошибка. Когда документ «Word» или «Excel» защищают паролем, то сколько бы текст файла не модифицировался, «RCA» всё время генерирует одну и ту же шифрпоследовательность.

Другими словами, если злоумышленнику удастся раздобыть больше одной (хотя бы две) версии зашифрованного документа, то раскрытие этого комплекта – уже дело техники.

В реальной жизни появление таких комплектов не редкость, поскольку при архивном копировании обычно сохраняется один из промежуточных вариантов файла, который находится в работе, а в организациях и офисах много документов создают и редактируют несколько людей, перенося варианты с одного компьютера на другой. Понятно, что эта ошибка фирмы «Microsoft» неслучайна и сделана в интересах АНБ.

Кроме того, АНБ подтвердила, что оказывала помощь в разработке безопасности ОС «Microsoft Windows Vista», чтобы защитить её от «червей», «троянских коней» и других кибер-угроз. Как сказал руководитель одного из подразделений АНБ Тони Сэйджер, принимавших участие в работе, «нашим намерением было помочь всем в обеспечении безопасности».

В АНБ отказались давать комментарии о своей работе в сфере кибербезопасности с другими компьютерными фирмами, но отметили, что «Microsoft» – единственная компания, с которой есть «такого рода отношения, когда факт сотрудничества признаётся при всём народе».

По свидетельству представителей спецслужбы, помощь «Microsoft» была бесплатной, а идея о публичном признании участия АНБ в разработке «Vista» исходила от корпорации.

Что касается защиты информации, важнейшая, по-видимому, особенность ОС «Vista» – это криптографическая подсистема «BitLocker» (для версий «Ultimate» и «Business»), которая даёт пользователям возможность шифровать все данные на «винчестере» и уже получила репутацию чрезвычайно надёжного средства.

По свидетельству известного эксперта Росса Андерсона, который выступил перед членами британского парламента, без секретного «чёрного хода» системы у компетентных британских органов практически нет шансов получить доступ к данным в компьютерах преступников, если там есть «BitLocker».

Кроме того, АНБ уже добралось и до систем защиты банковских сетей. Когда компания «MasterCard International» разрабатывала стандарт шифрования «SET», который используется сегодня в электронных транзакциях, АНБ быстро «остудило» её энтузиазм.

«Они сообщили нам, что можно и что нельзя делать», – сказал Джон Ванкмюллер, отвечавший в компании за электронную коммерцию. АНБ настояло на том, чтобы большая часть информации при каждой транзакции вообще не шифровалась, поскольку хочет знать, кто и куда переводит деньги.

По данным Эдварда Сноудена на сотрудничество со спецслужбами пошли многие крупные компании, предоставив им доступ к своим серверам. Среди них «Microsoft» (Hotmail), «Google» (Google Mail), «Yahoo!» и «Facebook», «AOL», «Apple» и «Paltalk».

«Skype» (600 миллионов пользователей и каждый третий международный звонок на планете) сотрудничала с АНБ ещё до покупки софтверным гигантом, позволяя прослушивать разговоры. «Microsoft», заполучив «интернет-телефон №1» в 2011 году, сильно переработала внутреннюю структуру сети, перенеся нагрузку с клиентов на собственное «облако».

Сказали, что это было необходимо, чтобы нормально использовать «Skype» на мобильных устройствах, но вместе с тем позволило контролировать пользовательский трафик. Так что, если раньше АНБ могло в лучшем случае вести аудиозапись переговоров, то теперь ей доступно и изображение.

Секретные документы, раскрытые Сноуденом, доказывают, что АНБ и британская ШКПС дискредитировали гарантии, которые провайдеры предоставляли своим клиентам, обещая им, что их онлайн-переписка, банковские операции и медицинская информация защищены от проникновения со стороны преступников и правительств.

Спецслужбы разработали целый ряд методов в ходе своего систематического, непрекращающегося наступления на то, что они считают главной угрозой для их способности отслеживать гигантские объёмы интернет-трафика – на повсеместное использование шифров в интернете.

Представители агентств настаивают на том, что способность взламывать шифры является основой их главной миссии, которая заключается в борьбе с терроризмом и сбором данных для внешней разведки. Однако эксперты в области безопасности обвинили их в том, что их деятельность представляет собой наступление на сам интернет и на неприкосновенность личной жизни его пользователей.

«Шифрование является основой доверия в интернете, – сказал Брюс Шнайер, специалист по шифрованию и сотрудник гарвардского Центра интернета и общества имени Беркмана. – Сознательно подрывая основы онлайн-безопасности с целью слежки, АНБ разрушает саму материю интернета».

На секретных брифингах представителей спецслужб США и Великобритании они празднуют свою «победу над безопасностью и личным пространством в сети». В одном из документов британской ШКПС 2010 года написано:

«В течение последнего десятилетия АНБ предпринимало агрессивные, многоэтапные попытки раскрыть технологии шифрования, широко используемые в интернете. Гигантские объёмы зашифрованных интернет-данных, которые до сегодняшнего дня мы были вынуждены обходить стороной, теперь пригодны к использованию».

В одной из внутриведомственных служебных записок говорилось, что, когда британским аналитикам, не посвященным в подробности программ АНБ, продемонстрировали успехи американских спецслужб, «они были потрясены».

Прорыв, о котором идёт речь и подробностей которого в документах нет, привёл к тому, что теперь секретные службы получили возможность отслеживать «большие объёмы» данных и взламывать их шифры, несмотря на то, что владельцы интернет-компаний продолжают уверять своих пользователей, что их личные данные защищены от проникновения со стороны правительственных структур.

Ключевым оружием борьбы АНБ с шифрованием стало взаимодействие агентства с техническими компаниями, подробности которого были изложены в сверхсекретном бюджетном запросе на 2013 год, поступившем от АНБ и носившего название «Активация радиоразведки» (англ. Sigint [signals intelligence] enabling).

Размеры финансирования этой программы – 254,9 миллиона долларов в 2013 году – намного превысили бюджет программы «PRISM», который составлял всего 20 миллионов долларов в год, о чём свидетельствовали другие документы АНБ. На протяжении 2011—13 годов на программу «Sigint enabling» было потрачено около 800 миллионов долларов.

В документах говорилось, что в рамках этой программы спецслужбы США «активно привлекают американские и иностранные технические компании, чтобы тайно или открыто влиять на разработку их коммерческой продукции». В документах не были указаны названия этих компаний.

Одной из целей этой программы являлось «закладывание слабых мест в коммерческие системы шифрования». Эти уязвимости были хорошо известны только АНБ в отличие от простых потребителей, которые в секретных документах названы «противниками», что весьма показательно. «Такие изменения структуры программы позволяют разведке использовать их для ведения наблюдения, поскольку им заранее известны все особенности модификации».

В секретных документах перечислялись основные цели программы, в том числе задача сделать коммерческие программы шифрования «более уязвимыми» для атак со стороны АНБ путем «придания нужной формы» мировому рынку, а также продолжающиеся попытки взлома шифров, которые используются в телефонах нового поколения «4G».

АНБ ожидало, что в 2013 году ему удастся получить доступ «к данным, передаваемым через узлы ведущих операторов связи», а также к «главной системе голосовой и текстовой связи между равноправными узлами».

В документах говорилось, что АНБ удалось достичь ещё одной цели, поставленной в бюджетном запросе: теперь спецслужбы имели возможность оказывать влияние на международные стандарты, на которых основывались системы шифрования. В одном из секретных документов, раскрытых Сноуденом, говорилось, что АНБ тайно разрабатывало свою собственную версию проекта стандарта безопасности, выпущенного Национальным институтом стандартов и технологии США и принятого во всём мире.

В документе говорится: «Проект „Bullrun“ направлен на расширение возможностей АНБ по взлому шифров, используемых в определенных технологиях передачи сетевой информации. В проекте принимают участие множество источников, все из которых засекречены». АНБ стали известны способы взлома наиболее широко используемых онлайн-протоколов, таких как

«https», «VoIP» и «SSL», которые призваны защищать банковские операции и покупки через интернет.

Этот документ также доказывал, что Центр коммерческих решений при АНБ, формально представлявший собой организацию, посредством которой компании могли проводить оценку своей продукции и предлагать её потенциальным правительственным покупателям, выполнял ещё одну, секретную функцию. АНБ использовало её, чтобы «устанавливать секретные партнёрские отношения с отдельными представителями индустрии» с целью «закладывать» уязвимости в производимые ими средства обеспечения безопасности.

Ещё в одной инструкции АНБ по обеспечению режима секретности содержались подробности тесного сотрудничества агентства с представителями индустрии, а также его возможностей в изменении характеристик продукции. Авторы инструкции предупреждали аналитиков о том, что сверхсекретными должны оставаться два факта.

Во-первых, что АНБ вносит изменения в коммерческие программы шифрования и устройства, чтобы «сделать их пригодными к использованию». Во-вторых, что АНБ «получает криптографические детали коммерческих систем обеспечения безопасности информации посредством связей с представителями индустрии».

Тем не менее, как говорилось в документе, АНБ пока не удалось взломать все технологии шифрования. «Шифры работают. Если их правильно использовать, мощные системы шифрования могут стать одной из немногих вещей, на которые вы действительно можете положиться», – сказал Сноуден, предупредив, однако, что АНБ может зачастую найти способ обойти эти системы из-за уязвимостей систем безопасности, установленных на одном из компьютеров, участвующих в коммуникации.

«Некоторые продукты, позволяющие нам вести наблюдение, применяются людьми в повседневной жизни, и некоторые слабые места, которыми тоже можно воспользоваться, хорошо всем известны, к примеру, можно легко узнать недостаточно надёжный пароль, – говорилось в документе. – Информация о том, что спецслужба использует эти продукты, а также о масштабах наших возможностей, повысит уровень осведомлённости общественности, что приведёт к нежелательному вниманию к нашей деятельности и деятельности наших политических руководителей».

«Лазейки в системах подрывают основы надёжной системы безопасности, – сказал ведущий технолог и старший аналитик Американского союза гражданских свобод Кристофер Согоян. – Такие лазейки подвергают всех пользователей такой системы, а не только объектов слежки разведслужб, повышенному риску раскрытия их личных данных. Так происходит, потому что внедрение лазейки в программу, особенно такой, которая позволяет получить незашифрованные данные и коммуникации пользователя, в значительной степени усложняет разработку безопасного продукта».

В результате раскрытия информации о тотальной слежке в интернете был зафиксирован всплеск интереса пользователей к различным технологиям шифрования хранящихся и пересылаемых данных (например, технология шифрования «PGP»), к использованию анонимного браузера «Tor» и зашифрованному аналогу электронной почты «Bitmessage». Так, в сети анонимайзера «Tor» в мае 2013 года количество запросов было относительно стабильным и составляло около 50 тысяч в сутки, однако с августа резко выросло до 120 тысяч.

Также значительно вырос рынок устройств, призванных помочь хранить данные пользователей в тайне. Если раньше подобные приспособления охотно покупали только крупные корпорации, то сегодня значительную часть клиентов составляют обычные пользователи и представители малого бизнеса. Компании, представляющие доступ к надёжной электронной почте, также увеличили количество своих пользователей в десятки и сотни раз. И это невзирая на то, что эти сервисы, в отличие от широко распространённых почтовых сервисов, являются платными.

Также, после скандала с обнародованием информации о программе «PRISM», «Google» приняла решение ускорить планы по внедрению сквозного шифрования между своими датацентрами по всему миру. Центры обработки данных компании размещены по всему миру, так, например, электронное письмо может храниться приблизительно в любом из 6 таких центров. Чтобы лишить правительство возможности контролировать линии передач данных между центрами, компания решила шифровать каждый бит пересылаемых данных.

Перехват информации с оптоволоконных каналов – не единственная проблема, которую нужно решать интернет-компаниям, если они хотят сохранить в неприкосновенности конфиденциальные данные пользователей. Ведь шифрование каналов связи может защитить только от прослушки оптоволокна, но не от прямого внедрения на серверы. Важно также разрабатывать и использовать новые мощные, а самое главное не скомпрометированные криптоключи.

Второе важное решение касается создания и тестирования технологии шифрования пользовательских файлов, хранящихся на сервисах компании. До сих пор и «Google», и многие другие интернет-компании осуществляли шифрование данных только при их пересылке. На самих серверах вся информация сохранялась незашифрованной. В целом, все эти меры призваны предотвратить возможность доступа к информации личного характера со стороны спецслужб и, соответственно, несколько улучшить репутацию компании.

Также следует отметить, что АНБ копалось не только в домашних компьютерах, но и в смартфонах. В результате всех шпионских скандалов стало известно, что спецслужбы запросто могли не только перехватывать телефонные звонки, но также достать из практически любого телефона ценную информацию, например, контакты из адресной книги, сообщения, и даже хранимые фото- и видеофайлы.

Согласно секретным докладам, за каждую ОС отвечала отдельная команда хакеров. Компанию «Apple» уже уличали в «подсматривании» за своими клиентами. Однако о таком размахе пользователи даже не подозревали. Спецслужбы могут перехватывать даже сообщения «BlackBerry Messenger», а также взломали почтовый клиент «BlackBerry», который считался самым безопасным в мире.

Как долго клиенты «BlackBerry» находятся «под колпаком» точно неизвестно. Самые ранние упоминания в докладе относятся к 2009 году, когда специалисты «BlackBerry» поменяли схемы шифрования, и спецслужбы на время утратили доступ к пользовательским данным. Впрочем, через несколько месяцев им снова удалось восстановить слежку.

«Android», как открытая система, уязвима больше всех остальных. Однако при этом она предлагает и самое большое количество дополнительных программ. На волне разоблачений шпионской деятельности правительств, было создано большое количество приложений для обеспечения безопасности смартфонов и планшетов под управлением «Android». Это и новые защищённые почтовые клиенты, и защищенные мессенджеры, и приложения шифрования файлов, и многое другое.

АНБ опровергает информацию СМИ о масштабах слежки за людьми, заявляя, что специалисты ведомства следят только за потенциальными террористами и преступниками. Однако Сенат США потребовал закрыть секретные программы, о существовании которых стало известно. Они считают, что сбор информации о телефонных разговорах миллионов граждан требует больших расходов и при этом не дает ощутимых результатов.

В 2013 году экс-директор ЦРУ Джон Бреннан выступил со следующим заявлением: «На протяжении истории нации использовали шифрование для защиты своих секретов, однако сейчас для сокрытия своей деятельности используют коды и современные террористы, и киберпреступники, и торговцы людьми и другие преступники. Наше управление должно этому противостоять, иначе оно не будет исполнять свои прямые задачи».

С одной стороны, спецслужбы должны обеспечить защиту своих граждан от действий террористов и преступников. С другой – все эти меры не должны нарушать права и свободы

личности. Государство, как инструмент обеспечения «общего блага», должно являться защитником прав и свобод человека от любых посягательств с чьей бы то ни было стороны, в том числе и со стороны самого государства.

4. Подразделение кибервойны

В январе 2010 года большое количество домовладельцев в городе Сан-Антонио (штат Техас) в недоумении остановились напротив закрытых дверей своих гаражей, поскольку они не открывались. Проблема, в основном, коснулась жителей города в районе Милитари Драйв и федеральной трассы, известной как «Loop 410».

Конец ознакомительного фрагмента.