ЭЛЕКТРОННЫЙ ШПИОНАЖ

Официальная учеба и секретная подготовка занимали все больше времени. Даже с Фабио удавалось пообщаться не каждый день. Однажды после занятий он неожиданно окликнул меня:

— Энтон, срочное дело, поехали.

Вопросы задавать не было времени. У входа уже рычала знакомая БМВуха.

— Сейчас едем на занятие по маскировке.

Машина, как и в прошлый раз, остановилась у здания медицинского факультета Университета Сан-Пауло. Вспомнились недавние анализы.

— Причем здесь маскировка?

Фабио не ответил, а, махнув электронным пропуском, протолкнул меня мимо входного турникета. Пять минут блуждания по коридорам — и мы перед дверью.

«Лаборатория медицинской техники. Посторонним вход воспрещен».

Фабио плюнул на свой большой палец и приложил его к матовой поверхности электронного замка. Дверь медленно отъехала. Мы вошли. Так же бесшумно она вернулась на место.

Тамбур два на два метра. Жутко! Тихое жужжание, как в рентгеновском аппарате.

Фабио прикладывает свой обслюнявленный палец к новому сканеру. Уф! Наконец-то выбрались.

Перед нами огромный зал с множеством экранов. Это точно не медицинская лаборатория.

— Фабио, где мы?

— В частном центре электронного мониторинга, который курирует мой папа.

К нам подошел седой интеллигентный мужчина, внешним видом и манерами схожий с ранним Джеймсом Бондом. Он уважительно поздоровался с Фабио и приветствовал меня по-русски, почти чисто.

— Здравствуй, Антон.

Фабио представил хозяина:

— Мистер Смит.

Подобное имя в сочетании со шпионской внешностью мистера Смита не оставляло сомнения, что его истинное имя мне никто сообщать не собирается.

— Энтон, следующая важнейшая тема — маскировка. Мистер Смит — эксперт в этой области. Подготовь свой мозг. То, что ты узнаешь, может взорвать сознание. Я здесь не в первый раз, но каждый раз поражаюсь уровню современных шпионских технологий.

Мистер Смит

— Садитесь, так будет проще, — сказал мистер Смит, — и расслабьтесь, будем беседовать.

Сейчас не двадцатый век, когда однажды попавший в поле зрения спецслужб агент мог переезжать из страны в страну, легализоваться на новом месте с новыми документами и шпионить дальше в свое удовольствие на пользу своей державе.

В наше время залог длительной работы, жизни и здоровья только в одном: никогда, даже случайно, не попадать в поле зрения спецслужб. Это непросто, учитывая, что сто процентов всех наших электронных коммуникаций, включая телефон и Интернет, контролируются, отслеживаются и анализируются.

Достаточно в частном разговоре или в электронном письме упомянуть некоторые слова, например, «бомба», «терроризм», «Бен Ладен», «оружие», и даже вроде совершенно безобидные «Обама», «Путин» или просто название спецслужбы: ЦРУ, ФБР, АНБ, Моссад, КГБ — все, включается система полного мониторинга и глобального анализа всех связей: твоей телефонной книги, списка контактов электронной почты, всех записей в социальных сетях, и не только твоих, но и всех твоих друзей.

Если один из них такой же шутник, или реальный агент, или оппозиционный деятель, то ты навсегда попадаешь в

список подозрительных лиц и можешь быть уверен, что до конца жизни останешься под колпаком.

— А если поменять телефон?

— Если обычный телефон или сим-карту ты поменяешь на другие такие же, это ничего не изменит. АНБ и другие государственные службы имеют доступ к сетям всех мобильных операторов и программное обеспечение для отслеживания местоположения всех имеющихся в мире мобильников, распознавания голосов и смысловой обработки речевых сообщений, причем практически на всех языках.

— И на русском?

— И на русском.

Помимо государственных, есть и частные спецслужбы. Собственно я возглавляю одну из них.

— Они могут прослушивать любого человека?

— Да.

— И даже президента?

— Даже.

Я, честно говоря, подумал, что это шутка. Сегодня же первое апреля. Но я не в России, никто сегодня еще не прикололся.

— А где сейчас наш президент? — спросил я, еще не настроенный на ироническую волну.

Мистер Смит сделал некие манипуляции на своем планшетнике и подвел меня к карте.

На все увеличивающейся карте Великобритании появился Лондон, еще крупнее – старинный особняк в центре города.

— Это фокус?

— Нет, это место нахождения айфона вашего президента. А так как они никогда не расстаются, полагаю, и президент рядом. Теперь посмотрим адресную книгу его телефона.

Так, из 93 контактов 8 находятся практически в этой же точке.

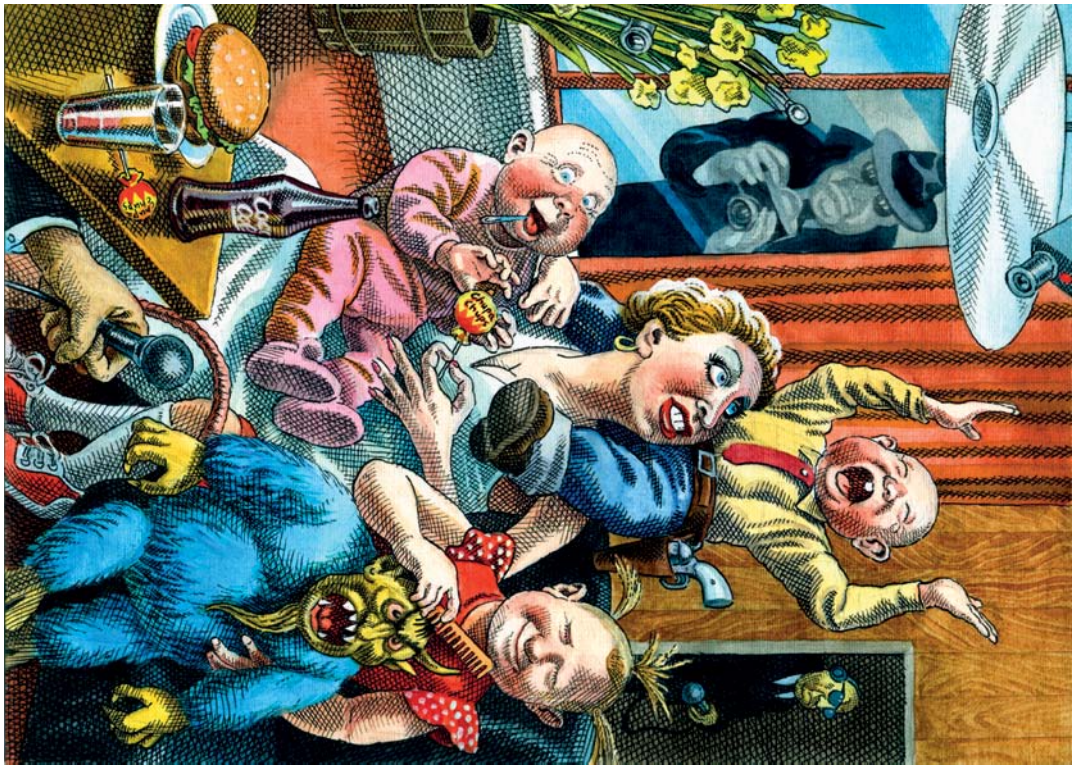
— А что они там делают?

— Для этого не надо прибегать к техническим средствам. Смотри иногда телевизор. Сегодня в Лондоне открывается международный саммит «большой двадцатки»*.

** Большая двадцатка, G20, группа двадцати — формат международных совещаний министров финансов и глав центральных банков, представляющих 20 экономик: 19 крупнейших национальных экономик (включая США, Россию, Бразилию) и Европейский союз.*

— Так, а почему члены русской делегации телефоны не выключат?

Не попадать в поле зрения спецслужб



— Ты меня спрашиваешь? У русских есть своя служба безопасности. Вопросы к ним.

— Можно послушать, о чем наши говорят между собой по телефону?

— Не только по телефону, можно слушать, что происходит на расстоянии до десяти метров от них, даже при выключенном девайсе.

Меня так и распирало от причастности к этому могуществу.

— Мистер Смит...

— Нет, слушать мы не будем, — предугадал он мой невысказанный вопрос, — излишнее любопытство, не вызванное особой необходимостью, противоречит шпионской этике.

— Как это?

— Ну, например, американская система «Эшелон»*. С её помощью сотрудники системы периодически следят за своими женами и детьми... Начальники их иногда ловят и наказывают. Но многие все же не могут отказать себе в удовольствии использовать служебное кибермогущество в личных целях. Это и есть одно из нарушений шпионской этики. Без необходимости мы не имеем права вторгаться в личную жизнь.

** «Эшелон» — общепринятое название глобальной системы радиоэлектронной разведки, работающей в рамках соглаше-*

ния о радиотехнической и разведывательной безопасности Великобритании, США и нескольких других стран. «Эшелон» имеет возможность перехвата и анализа телефонных переговоров, факсов, электронных писем и других информационных потоков по всему миру путём подключения практически ко всем каналам связи.

— У вас есть необходимость слушать президентов?

— В разведке не принято задавать лишних вопросов. Но подумай сам, Бразилия — член «двадцатки». «Двадцатка» — это не союз единомышленников, а просто толпа представителей двадцати геополитических противников. У нас есть долг и ответственность перед своим народом и государством. Если мы не будем знать планы противников, мы не сможем эффективно противостоять угрозам.

Американцы сами признаются, что деятельность АНБ, связанная с международным коммерческим шпионажем, позволила в прошлом году пополнить американскую казну на 16 миллиардов долларов, основная часть которых приходится на контракты, выигранные американскими корпорациями.

— Пополнить за чей счет?

— В том числе, и за бразильский. Это справедливо? Если мы сможем отыграть хотя бы один миллиард у аме-

риканцев – это будет по-честному. Ибо честность в геополитике имеет совсем иное значение, чем честность в обычных человеческих отношениях.

— Но у Бразилии, наверное, есть и друзья в «двадцатке».

— Друзья и союзники — это разные понятия. Вспомни высказывание Уинстона Черчилля: «У Британии нет постоянных врагов и постоянных друзей, а есть только постоянные интересы». Это главная идея, которой должны руководствоваться все государства и их руководители. «Друзья» тоже не прочь урвать за счет Бразилии, а значит, и её народа, миллиард-другой. Но мы тоже не ликом шиты.*

** «Не лыком шит» - русская поговорка. Сейчас используется в смысле «не такой уж он простой, как кажется».*

— Помимо глобальных систем электронной разведки, существует целый ряд специальных систем и устройств для слежения за отдельными гражданами.

— Сколько систем?

— Сразу ты все равно не запомнишь, поэтому попробуй применить мнемоническое правило. При описании каждой системы или шпионской технологии ты будешь загибать и считать пальцы. Только тебе придется представлять и то, как ты загибаешь пальцы ног. Готов?

Я сосредоточился.

1. Наблюдательные программы Агентства национальной безопасности.

Фактически, все электронные сообщения (электронные письма, факсы и звонки) в США отслеживаются гигантской сетью АНБ, которое было специально создано для анализа всех информационных потоков. Существует система наподобие Google, но значительно более мощная, которая в реальном времени может искать любую информацию по многочисленным запросам, таким как телефонные номера, ключевые слова, страны или абоненты.

2. Определение местонахождения человека по излучению его мобильника. Даже когда он выключен.

3. Можно отследить все перемещения абонента и все его действия с телефоном. Ну и, разумеется, такие «мелочи», как прослушивание его разговоров и чтение его Интернет-трафика.

4. Программное обеспечение, которое сможет записывать, сохранять и распознавать миллионы голосов. Для русского языка программа разработана в России в Центре речевых технологий. За три секунды она способна проанализировать более 10 000 вариантов различных голосов и сравнить их с образцами.

— Не понял. Что, русские делают программы для американских спецслужб?

— Нет, делали они в надежде продать в России. Не удалось. Чем американцы, естественно, воспользовались.

5. Дистанционное сканирование телефонных книг мобильников. Это делается при контроле в крупнейших аэропортах США и Европы.

— А в России? Знаете?

— Знаю, но не скажу.

6. Дистанционное сканирование информации с банковских пластиковых карт. Дороговатая техника, но вполне доступная не только государственным спецслужбам, но и преступным группировкам.

7. Удаленные сканеры, которые смогут сканировать людей с расстояния в 50 метров. Сканнер уже способен сканировать тело, одежду и багаж с дистанции в десятки метров. Устанавливается в аэропортах и пограничных пунктах контроля. В основе технологии лежит лазерное сканирование на молекулярном уровне. О человеке становится известно сразу все: от микроскопических следов наркотических веществ или порохового нагара на одежде, до уровня адреналина в крови и содержимого желудка. Причем, сам человек о своем «обследовании» не будет даже подозревать.

8. Видеокамеры. Наиболее широкая сеть полицейских видеокамер находится в крупных городах США. Эта система рассчитана не только на опознание преступников, но и на

их поимку во время совершения преступления. Данные всех видеокамер поступают в командный центр, чей компьютер оснащен мощной аналитической программой, способной работать в режиме реального времени. К системе имеют доступ также другие организации, такие как ФБР и АНБ.

9. Технологии распознавания человеческих лиц. Сегодня уже в 40 американских штатах используются подобные технологии при фотографировании на водительские права. Именно поэтому существуют строгие указания, где нужно делать такое фото — чтобы лицо было занесено в базу данных. Но не только госслужбы заняты этим. Большие частные компании, такие как Disney, тоже заинтересованы в том, чтобы считать по головам людей, посещающих Диснейлэнды, для дальнейшего маркетингового использования этих данных. Технология вышла из-под контроля и угрожает простым гражданам с самых разных сторон.

10. Автоматические распознаватели автомобильных номеров. В большинстве развитых стран уже развернута сеть камер, оснащенных специальным программным обеспечением, умеющим распознавать автомобильные номера. Это сделано для того, чтобы отслеживать угнанные машины, а также перехватывать скрывающихся преступников. Но возможности этой системы, разумеется, значительно шире — ведь теперь можно отследить и проанализировать

перемещения любого автовладельца в пределах города, а в перспективе — и всей страны.

11. Технология «предугадывания» преступлений. Существуют специальные алгоритмы, позволяющие превратить видеокамеру в устройство, распознающие признаки готового вот-вот совершиться преступления. Пилотный проект был запушен в Сан-Франциско, где камеры расположили в трамваях, автобусах и метро (по 12 камер на каждой из 22 станций). Камеры могут одновременно следить за 150 людьми в реальном времени и моментально замечать «подозрительное поведение».

12. Мобильные сканирующие рентгеновские установки. Мобильные сканирующие установки уже давно ездят по дорогам, неотличимые от обычных авто, и удаленно просвечивают движущиеся машины и людей, видя все, что находится у них внутри. Помимо рентгеновских установок, существуют аналогичные приборы на быстрых нейтронах*, которые позволяют выявлять атомный и химический состав грузов. Естественно, попавших под радиоактивный обстрел людей никто не спрашивает об их согласии.

**Такие нейтроны возбуждают ядра вещества. В результате, под действием быстрых нейтронов объект досмотра начинает «светиться» — излучать гамма-кванты с определенными энергиями. Это «свечение» индивидуально для каждого эле-*

мента и именно по характеру спектра гамма-квантов можно определить, как много в веществе того или иного элемента.

13. Моментальный тест ДНК. Это то, что спецслужбы любят даже больше, чем технологии распознавания лиц. Мобильные устройства для моментальной ДНК-идентификации — это быстрый путь к безошибочному распознаванию преступника. Для того, чтобы анализатор мог распознать образец ДНК, ему подойдет любой фрагмент из личных вещей.

14. Новое поколение идентификационных систем ФБР. ФБР завершает создание самой всеобъемлющей базы данных на всех жителей США, в которую войдет вся возможная информация о каждом. Здесь будет все: от отпечатков пальцев до биометрических данных и электронной слежки за коммуникациями человека. При такой системе любой не внесенный в базу человек сразу становится объектом особого внимания.

15. Помимо камер обычных, видимых, вокруг американцев существует огромное количество камер скрытых, о существовании которых они и не подозревают. Эта сеть носит название TrapWire. Камеры расположены вокруг «объектов особой важности» и реагируют на определенные действия — фотографирование объекта, частые появления вокруг него и прочее. Так человек, сам того не по-

дозревая, может попасть в разряд готовящих теракт преступников.

16. Есть еще целый ряд программ, разработанных и используемых американским Агентством национальной безопасности, которые позволяют собирать огромное количество личных данных пользователей компаний, предоставляющих услуги доступа в Интернет. Речь идет обо всех крупнейших социальных сетях и сервисах Youtube, Google, Yahoo, Skype ...

— А о русской социальной сети «В контакте»?

— Естественно!

17. Кстати, смартфоны могут заносить в системные поля фотофайла координаты точки, в которой сделан снимок. При публикации снимка в социальных сетях онлайн-ресурсы могут автоматически сопоставить координаты и выдать точный адрес места съемки.

Я добросовестно мысленно попытался загнуть семнадцатый палец — указательный на правой ноге.

Мистер Смит, видимо, почувствовал, что пора заканчивать.

— Какой из всего этого вывод? Девяносто процентов всех данных человек сам раскрывает для желающих за ним следить, из них большую часть по собственной беспечности, купившись на пряник по имени «куки».*

Паранойя

** Термин «куки» (печенье) происходит от английского «cookie» — набора данных, которые программа получает и затем отправляет обратно на сервер неизменными. Куки значительным образом влияют на конфиденциальность и анонимность пользователей Интернета.*

Я почувствовал себя голым и растерянным. Пропала даже иллюзия какой-то приватности.

— Мистер Смит, как это все запомнить и как с этим бороться?

— Лучше не бороться, а избегать контакта с возможными угрозами. У правоверных евреев имеется, в отличие от христиан, не 10, а 613 заповедей. Тора советует избегать упомянутых в заповедях грехов. Я думаю, с этим непросто жить. Надо просто привыкнуть. Шютка!

Последнее слово мистер Смит тоже произнес по-русски.

ПРОТИВ ПАРАНОЙИ

Мистер Смит был, наверное, не только техническим спецом, но и классным психологом.

Две недели я осмысливал услышанное и увиденное.