

Вадим Гребенников

Стеганография. История тайнописи



ЛитРес: Самиздат
Москва

УДК 82-3
ББК 68
Г79

Гребенников В.

Стеганография. История тайнописи / В. Гребенников —
Москва: ЛитРес: Самиздат, 2019. — 142 с.

ISBN 978-5-5321-0646-8

В отличие от криптографии, которая шифрует содержимое секретного сообщения, стеганография скрывает сам факт его существования. При этом ее можно совмещать с методами криптологии, усложняя в целом систему защиты информации. Книга рассказывает историю рождения и эволюции стеганографии в мире, разработки и усложнения методов и средств скрытой тайнописи: невидимые чернила, маскировка и микроточки, а также описывает современные цифровые стеганографические технологии и кибератаки.

ISBN 978-5-5321-0646-8

© Гребенников В., текст, 2019
© Omiko Trading LTD., оформление, 2019

Введение

С возникновением письменности задача обеспечения секретности и подлинности передаваемых сообщений стала особенно актуальной. Действительно, сообщение, переданное словесно или показанное жестами, доступно для постороннего только в тот краткий промежуток времени, пока оно «в пути», а в его авторстве и подлинности у получателя никаких сомнений быть не может, потому что он видит своего собеседника.

Иное дело, когда сообщение записано – оно уже живет отдельной жизнью и имеет свой путь, зачастую далеко расходящийся с путем человека, его создавшего. Записанное на бумаге сообщение существует в материальном мире гораздо более длительный промежуток времени, и у людей, желающих ознакомиться с его содержанием против воли отправителя и получателя, появляется гораздо больше шансов сделать это.

Поэтому именно после возникновения письменности появилось искусство тайнописи, искусство «тайно писать» – набор методов, предназначенных для секретной передачи записанных сообщений от одного человека другому. Данные о первых способах тайнописи весьма обрывочны. Предполагается, что она была известна в древнем Египте и Вавилоне.

При этом тайнопись делилась на два вида: шифрование (криптография) и сокрытие информации (стеганография). Слово «стеганография» происходит от греческих слов «steganos» – скрытый и «graphein» – писать.

Стеганография – это мероприятия по сокрытию и защите информации, а стегоанализ – это мероприятия по разбору и раскрытию тайной информации. Вместе стеганография и стегоанализ создают науку стеганологию (греч. λόγος – слово, понятие). Стеганология – это наука об использовании всех доступных средств (невидимые чернила, микроточки, маскировка, компьютеры) для сокрытия и раскрытия тайной информации.

Криптография изучает методы сокрытия данных для хранения или передачи, причем данные преобразуются в форму сообщения, которое специально не скрывается, и допускается возможность его анализа противником. Цель классической стеганографии состоит в том, чтобы скрыть секретные данные в других открытых наборах или потоках данных таким способом, который не позволяет обнаружить, что в них имеется какая-то скрытая составная часть, и тем самым выделить эти сообщения среди остальных.

Поэтому можно было бы сказать, что стеганография – это искусство и наука о способах передачи (хранения) сообщений, скрывающих факт существования скрытого канала связи (скрываемых данных).

Стеганографию следует отличать и от сигнальных систем. С древних времен применяется метод сокрытия данных, который основан на построении некоторой сигнальной системы с использованием «условных знаков», т.е. не привлекающих внимание знаков и сообщений, смысл которых оговорен заранее и держится в секрете. С их помощью одна из сторон может передавать другой короткие сообщения о ходе событий или интересующих объектах, а также информировать другую сторону о том, какой способ поведения необходимо выбрать в данный момент.

В первый раз о стеганографии было упомянуто ещё в V веке до н.э. в летописи Геродота. В ней он рассказывал о вооружённых столкновениях между Грецией и Персией в V веке до н.э., которые рассматривал как противоборство между волей и рабством, между независимыми греческими государствами и Персией. Согласно Геродоту именно искусство тайнописи спасло Грецию от порабощения Ксерксом, «царем царей», правителем Персии.

Отношения между Грецией и Персией значительно обострились вскоре после того, как Ксеркс начал строительство города Персеполь, новой столицы своего царства. Дань и подарки поступали со всех концов империи и соседних государств, за исключением Афин и Спарты. Решив отомстить за такую дерзость, Ксеркс начал мобилизацию войска, заявив: «Мы так расширим персидскую империю, чтобы её границей служило небо, чтобы солнце не смогло увидеть

ни лоскутков земли за нашими границами». Следующие пять лет он потратил на то, чтобы тайно собрать наибольшую в истории армию, и в 480 году до н.э. уже был готов нанести внезапный удар.

Однако наращивание военной силы Персии видел Демарат, грек, изгнанный из родины и живший в персидском городе Сузы. Несмотря на изгнание, он всё же оставался лояльным к Греции и потому решил предупредить спартанцев о плане вторжения Ксеркса. Проблема заключалась лишь в том, как передать сообщение, чтобы его не смогли перехватить персидские солдаты. Геродот писал так:

«Поскольку опасность обнаружения послания была очень велика, то оставался только единственно возможный способ, которым Демарат мог успешно передать своё послание. Он соскоблил воск с двух сложенных дощечек для письма, написал прямо на дереве, что собирается делать Ксеркс, а затем снова покрыл воском дощечки с сообщением. По внешнему виду дощечки казались чистыми, без каких-либо записей, поэтому они не вызывали подозрения у персидских солдат.

Когда гонец с посланием добрался до места назначения, никто не мог и предположить о наличии послания, пока, как я полагаю, дочь Клеомена [царя Лаконики в 520-491 г.г. до н.э.], Горго, которая была женой Леонида I [царя Лаконики в 491-480 г.г. до н.э.], не догадалась и не сказала другим, что если они счистят воск, то найдут записанное под воском на дощечках послание. Так и сделали; после того как был счищен воск, под ним обнаружилось послание, которое прочли, а затем передали в другие греческие города».

Благодаря этому предупреждению беззащитные на тот момент греки стали сами вооружаться. Доходы от надлежащих государству серебряных рудников, которые до этого распределялись среди граждан, были направлены на строительство двухсот военных кораблей.

В результате Ксеркс потерял элемент внезапности, и 23 сентября 480 года до н.э., когда персидский флот достиг Саламинского пролива неподалёку от Афин, греки уже были наготове. Хотя Ксеркс думал, что он поймал греческий флот в ловушку, но в действительности греки сознательно заманивали персидские корабли в пролив. Греки знали, что их небольшие суда, которых к тому же было в

несколько раз меньше, чем у персов, в открытом море будут уничтожены, но внутри пролива, благодаря маневренности, они смогут победить персов.

Поскольку ветер изменил направление, то персидский флот оказался внутри пролива и вынужден был принять бой на греческих условиях. Корабль персидской царицы Артемисии был окружён с трёх сторон, так что она смогла вырваться назад в море, только протаранив один из своих кораблей. Возникла паника, большое количество персидских судов сталкивались друг с другом, и греки начали стремительную атаку. В течение одного дня флот персов был уничтожен.

Геродот также вспомнил ещё об одном случае, когда сокрытие послания оказалось достаточным, чтобы беспрепятственно его передать. Он рассказал историю о Гистии, который хотел подтолкнуть Аристагора и Милета к восстанию против персидского царя Дария. Чтобы послания не обнаружили враги, Гистий побрил голову своего вестника, написал на коже текст послания, а затем подождал, пока волосы не выросли опять. Что же, неспешный в то время ход истории позволял пользоваться такими способами. Посланец, у которого не было ничего явно его компрометирующего, мог путешествовать, не беспокоясь. По прибытии на место он побрил голову и «вручил» послание адресату.

Заметным вкладом в стеганографию в 357 году до н.э. стал «книжный шифр» древнегреческого полководца Энея Тактики, описанный им в трактате «О перенесении осад». В разделе «О тайных письмах» Эней предложил прокалывать малозаметные дыры в книге или в другом документе над буквами (или под ними) секретного сообщения. Интересно отметить, что в Первой Мировой войне германские шпионы использовали аналогичный способ сокрытия секретных писем, заменив дыры на точки, которые наносились симпатическими чернилами на буквы газетного текста.

Древние китайцы использовали следующий вид стеганографии: писали сообщение на тонкой шёлковой ткани, которая потом свёртывалась в крошечный шарик и покрывалась воском. Посланец глотал этот восковой шарик и в своём желудке доставлял послание к опре-

делённому месту, где естественным путём оно изымалось и передавалось адресату.

То, что стеганография смогла просуществовать столь длительное время, показывает, что она, несомненно, обеспечивает определённую секретность, но ей свойствен один принципиальный недостаток. Если курьера обыскают и найдут сообщение, то сразу же станет известно и его содержание. Перехват сообщения мгновенно ставит под угрозу всю безопасность. Пристальная стража может тщательным образом обыскивать всех, кто пересекает границу, счищая с дощечек весь воск, нагревая чистые листы бумаги, очищая сваренные яйца от скорлупы, брея людям голову и т.д., так что случаи выявления сообщения будут неминуемы.

Следующий рукописный труд о стеганографии появился только в конце XV века. Так, в 1499 году Иоганн Тритемий (Трисемус), аббат бенедиктинского монастыря Святого Мартина в Шпанхейме (Германия), приступил к написанию серии томов под общим названием «Стеганография» (лат. *Steganographia*). В первых разделах он писал о способах замены гласных-согласных, о криптографическом использовании «пустых» знаков и не имеющих смысла слов. Но из-за ереси, что по мнению христианских священников содержалась в произведении, он продолжительное время оставался в виде рукописи. А после того, как в 1606 году книга всё же была напечатана, она сразу была внесена в католический Индекс запрещённых книг.

В 1682 году Генрих Хиллер написал книгу «Глубочайшая тайна стеганографических искусств» (лат. *Mysterium artis steganographicae novissimum*), в которой намеревался научить читателя не только тайнописи, но и распознавать такие языки, как латинский, немецкий, итальянский и французский, просто определяя статистическую частоту букв и дифтонгов (сочетание двух простых гласных).

В дальнейшем стеганографическими методами сокрытия своей переписки очень часто пользовались русские революционеры. Так, в 1902 году в Женеве в типографии «Союза русских социал-демократов» была издана брошюра Владимира Петровича Акимова (наст. фам. Махновец) «О шифрах», где во второй главе «Как спрятать шифр» были описаны химические методы тайнописи для революци-

онеров-подпольщиков. В брошюре В.П. Акимов пояснил, что наиболее надёжным средством являются невидимые чернила, реагирующие только на определённый химический состав.

1. История стеганографии

1.1. Невидимые чернила

В некоторых способах стеганографии использовали физические особенности носителей информации. Так, симпатические, т.е. невидимые, чернила исчезали вскоре после написания ими текста или были невидимы с самого начала. Они представляли собой химические растворы, которые становились бесцветными после высыхания, но видимыми после обработки другим химикалием (реагентом).

Например, если писать железным купоросом, то текст является невидимым, пока его не обработают раствором цианата калия, после чего образуется берлинская лазурь – вещество, имеющее прекрасный цвет. Искусство изготовления качественных чернил для тайнописи заключалось в том, чтобы найти вещество, которое бы реагировало с минимальным количеством химикалий (лучше всего лишь с одним).

Невидимые чернила были двух видов: органические жидкости и «симпатические» химикалии. Первые, к которым относятся моча, молоко, уксус и фруктовые соки, становятся видимыми в результате незначительного нагревания. Вторые – в результате обработки бумаги специальным химическим реактивом или освещения лучами определённой части спектра, обычно, ультрафиолетом.

Этот способ стеганографии получил свое начало с незапамятных времён. Еще китайский император Цин Шихуанди (249-206 г.г. до н.э.) использовал для своих секретных писем густой рисовый отвар (удерживающий крахмал), который после высыхания написанных иероглифов не оставлял никаких видимых следов. Если такое письмо слегка смачивали слабым спиртовым раствором йода (или отваром водорослей), то появлялись синие надписи.

Римский учёный Плиний-старший в своей «Естественной истории», написанной им в I веке до н.э., рассказывал, каким образом

можно использовать сок растений из семьи молочаев в качестве симпатических чернил. После высыхания надпись, сделанная этими чернилами, была не видна, но при слабом нагревании становилась коричневой.

Много органических жидкостей ведут себя похожим образом: при нагревании, из-за того, что в них содержится большое количество углерода, они темнеют. И это известно подготовленным шпионам, которые в случае окончания симпатических чернил используют для этой цели собственную мочу.

Великий римский поэт Публий Овидий Назон, который жил в I веке до нашей эры, в поэме «Наука любви» рекомендовал влюблённым способ тайнописи молоком, проявляемой посыпанием бумаги сажеей. После сдувания сажки на бумаге оставались её мелкие частицы, прилипшие к местам, где были написанные молоком буквы.

В I веке нашей эры Филон Александрийский описал способ изготовления «тайных» чернил из сока чернильных орешков с последующей обработкой написанного раствором железомедной соли.

В 1412 году несколько видов симпатических чернил описал арабский криптолог Шехаб аль-Калкашанди (1355-1412) во второй части раздела под общим заголовком «Относительно сокрытия в буквах тайных сообщений» своей «Энциклопедии всех наук».

В 1558 году итальянский криптолог Джованни Баттиста делла Порты (итал. Giovanni Battista della Porta, 1535-1615) посвятил вопросу невидимой переписки отдельную книгу «Магия естественная» (лат. *Magia naturalis*). Он описал, как спрятать послание внутри сваренного вкрутую яйца, сначала изготовив чернила из одной унции (28 г) квасцов и пинты (0,5 л) уксуса, а затем написав послание этими чернилами на скорлупе. Раствор проникал сквозь поры скорлупы и оставлял сообщение на поверхности плотного яичного белка, которое можно было прочитать, только разбив яйцо и очистив скорлупу.

Название «симпатические чернила» было введено в конце XVII века химиком Лемортом из Лейдена. Он дал это имя водному раствору «свинцового сахара». Так называлась укусно-свинцовая соль