

Документ и информационная безопасность: прошлое и настоящее

И.А. Русецкая

Вклад Иоанна Тритемия в развитие европейской криптографии (К 555-летию со дня рождения)

Статья посвящена оценке роли и значения трудов мыслителя раннего Нового времени Иоанна Тритемия (1462–1516), внесшего большой вклад в развитие европейской криптографической мысли.

Ключевые слова: Иоанн Тритемий, криптография, раннее Новое время.

Во все эпохи своего существования криптография была важна для написания тайных посланий. У европейских интеллектуалов раннего Нового времени появилась еще одна причина для проявления внимания к тайнописи. В этот период на ее теорию и практику значительно повлиял возросший интерес к каббале и неогерменевтическим учениям. Это направление развивалось независимо от существующих традиций применения методов криптографии, в частности в дипломатии¹.

Исследователем, первым отразившим подобный взгляд на вопросы тайнописи, явился Иоанн Тритемий, сочинение которого «Стеганография», посвященное данной проблеме, нашло в то время многих последователей. В труде Тритемия отразилось увлечение автора практической каббалой, но с точки зрения криптологии интерес представляют элементы описания и применения методов криптографии, часть из которых являлась новаторской.

Тритемий (1462–1516), настоящее имя которого Иоанн Гайденберг, был историком, гуманистом, религиозным деятелем. Он родился недалеко от Трира в Германии в небольшом городке Триттенхайм, по названию которого взял себе псевдоним. Он был монахом, а затем настоятелем Шпонгеймского бенедиктинского

монастыря Св. Мартина, знаменитого своей обширной библиотекой. На склоне лет Тритемий стал аббатом Шотландского монастыря Св. Иоанна.

Разносторонняя направленность его многочисленных сочинений и их энциклопедическое содержание позволяют поставить Тритемия в один ряд с видными германскими гуманистами.

С вопросами тайнописи связаны два сочинения из большого письменного наследия автора: «Стеганография» и «Полиграфия».

В 1500 г. Тритемий написал две первые книги своей работы «Стеганография», которая создала ему на долгие годы репутацию оккультиста. Так, в 1606 г. это произведение было включено в индекс запрещенных книг².

Непосредственно повлиял на интерес Тритемия к этой тематике, вероятно, Либаний, теолог и врач³. Он встречался с Тритемием в Шпонгейме в 1494 г. Тритемий был также лично знаком с Агриппой Неттесгеймским (1486–1535) и с работами Рейхлина, посвященными каббале.

Оригинал рукописи «Стеганографии» был, по всей видимости, уничтожен, но текст его был переписан и сохранен. По свидетельствам Джордано Бруно, Джона Ди, Агриппы Неттесгеймского и других поклонников работы Тритемия в XVI в., т. е. до того, как «Стеганография» была издана, ее содержание стало известно в Европе среди достаточно широкого круга читателей⁴. Известный французский криптограф и дипломат Блез де Виженер в своем «Трактате о шифрах», посвященном криптографии, указывает на знакомство с несколькими рукописными вариантами труда Тритемия, при этом отмечая, что ему не удалось установить, каково криптографическое наполнение третьей книги «Стеганографии»⁵.

Первое издание «Стеганографии» было напечатано в 1606 г. во Франкфурте. Кроме собственно «Стеганографии» издание содержало еще две работы, имеющие отдельные названия и нумерацию: *Clavis Steganographiae*; *Clavis generalis*⁶.

Текст «Стеганографии» можно также прочесть в работе Вольфганга Эрнста Хайделя, соратника майнцского архиепископа, выходившей в свет в 1676 и 1721 гг. соответственно в Майнце и Нюрнберге⁷. Помимо текста «Стеганографии», процитированного по изданию 1621 г., в этой работе приведена биография Тритемия и рассмотрены криптографические методы, применявшиеся им в первых двух книгах «Стеганографии». В.Э. Хайдель предпринимает анализ криптографического содержания трактатов «Стеганография» и «Полиграфия».

В 1498–1499 гг. Тритемием также была составлена версия, известная под названием *Clavis specialis Steganographiae*. Окончательный сохранившийся вариант «Стеганографии» был усовершенствованным в 1499–1500 гг. вариантом *Clavis specialis*, который сам по себе так и не был издан.

Значение этой версии для раскрытия шифров, примененных Тритемием в «Стеганографии», читателям удалось оценить только в 1601 г., когда под именем Густава Селена герцог Брауншвейгский и Ганноверский Август Второй выпустил работу, посвященную истории тайнописи и описанию известных систем шифрования⁸. Одну из девяти книг своего труда Селен отвел оценке вклада Тритемия в криптографию.

Далее рассмотрим, чему посвящено основное содержание трех книг «Стеганографии» Тритемия.

Первая часть включает в себя тридцать две главы, в которых описываются иерархии духов, каждый из которых действует в определенной сфере жизни: в торговле, политике, частной жизни и т. д. Письма, имеющие невинное содержание, позволяют передавать адресату некоторый тайный смысл при помощи того или иного духа, отмечающего письмо определенным символом.

Вторая часть «Стеганографии» содержит двадцать пять глав, каждая из которых, кроме заключительной, посвящена описанию принципов передачи на расстояние мысленных посланий в соответствующий час суток.

Из третьей части «Стеганографии» до нашего времени дошла лишь первая из 7 глав. Она посвящена описанию способов передачи тайных посланий на далекие расстояния при помощи астрологии. Глава содержит восемь «астрологических» таблиц с цифрами, символами астрологии и греческими буквами. Суть составления этих таблиц была непонятна большинству читателей книги.

Понять криптографическую составляющую «Стеганографии» становится легче при использовании *Clavis Steganographiae*. Эта версия дает возможность расшифровать содержание первых двух книг. В частности, это делает Селен в своей работе. Использованные Тритемием шифры являются сравнительно несложными шифрами простой замены или перестановки, хорошо известными в то время; отдельные фразы шифруются несколько раз.

Третью часть «Стеганографии», однако, дешифровать таким образом некоторое время не удавалось, поскольку, несмотря на внешнее сходство ее содержания с тематикой предыдущих книг, *Clavis Steganographiae* не включала в себя соответствующих разъяснений. Это стало причиной различных толкований ее смысла.

Шифры третьей части были раскрыты в 1676 г. Хайделем и проанализированы в его упоминавшейся работе. Для дешифрования Хайдель использовал систему, описанную Тритемием в другом его труде, «Полиграфии», который и внес крупный вклад в развитие идей шифрования в раннее Новое время.

Уже в 1990-е гг. исследователь проблем криптологии Т. Эрнст описывает раскрытие шифра, использованного Тритемием в цифровых таблицах третьей книги⁹. Эрнст подтверждает точку зрения Хайделя о том, что Тритемий использовал в этой части своей работы нумерический шифр, основанный на принципах полиалфавитной замены букв цифрами, которая рассматривалась Тритемием в шестой книге труда «Полиграфия»¹⁰.

Реконструируя этот метод шифрования, Эрнст приводит в своей работе таблицу, позволяющую легко его использовать, в том числе, для обратной процедуры¹¹. Данный метод отличают следующие характерные черты:

- 1) использование вводящих в заблуждение «лишних» цифр, которые также несут функции разделения слов в предложении;
- 2) использование зодиакальных знаков, с одной стороны, для отвлечения внимания читателя, с другой стороны, для указания на смену использованного алфавита замены.

Развивая положения статьи Эрнста, следует указать, что такая таблица может быть составлена не только исходя из шестой книги «Полиграфии», но также из таблицы, которую можно обнаружить во вступлении к третьей части «Стеганографии». Последняя таблица включает имена духов различных категорий, которым соответствует тот или иной астрологический символ. В таблицах первой главы этот символ указывает на то, какая последовательность цифр используется для шифрования соответствующего отрывка. В качестве примера в конце таблицы зашифровано имя Тритемия, в котором каждой букве соответствует определенный набор из трех цифр.

В таблицах Тритемием были зашифрованы пять коротких предложений на латинском и немецком языках. В использованных шифрах применяется прогрессивная для того времени система шифрования, давшая впоследствии название соответствующей категории шифров – шифры многоалфавитной, или полиалфавитной, замены.

Эрнст считал, что «Стеганография» и «Полиграфия», по мысли Тритемия, должны были составлять единый труд. По мнению этого исследователя, это те самые книги, посвященные тайнописи, о которых их автор пишет в письме к Рогерию Сикамбру от 31 августа 1507 г., и во введении к «Полиграфии», посвященном императору

Максимилиану I¹². Таким образом, «Полиграфия» продолжает незаконченную «Стеганографию» и поясняет ее, позволяя восстановить метод шифрования, который приводится в «Стеганографии».

Такую точку зрения разделяли и другие исследователи работ Тритемия, например Шнееганс, указывавший на отсутствие серьезных отличий между двумя сочинениями, если не считать сознательно добавленного магического антуража¹³.

Слабым местом этой версии является то, что она может быть доказана лишь тем фактом, что Тритемий действительно собирался написать 8 книг, посвященных искусству тайнописи. Но в письме к Сикамбру Тритемий пишет о том, что из восьми книг будет состоять лишь «Стеганография». В письме же к монаху кармелитского ордена в Генте Арнольду Бостию в 1499 г. Тритемий упоминает, что планирует создать грандиозный труд, какого мир еще не видел; первой его частью будет «Стеганография». Всего же книг будет четыре и каждая будет содержать не меньше ста глав. На основании этого можно было бы предположить, что кроме «Стеганографии» Тритемий собирался написать еще три книги в продолжение этой темы. Однако это утверждение не может считаться доказанным, поскольку Тритемий, вероятно, много раз менял замыслы своих сочинений. Например, в письме к тому же адресату он писал, что первая часть его великого сочинения, иными словами, «Стеганография», будет включать описание более сотни методов передачи на расстояние тайных посланий. Во второй книге такие методы связывались с особым образом подготовленными помощниками-курьерами, которые смогли бы сохранить содержание секретного письма даже в случае использования пыток. Предполагалось описание и способа передачи письма без помощи курьера. Книга третья должна была включать описание методов, позволяющих человеку выучить за два часа латинский язык. Четвертую часть планировалось посвятить мысленному внушению содержания секретных писем и т. д. Логично было бы предположить, что такой план автор составил для большого труда, в качестве первой книги которого планировалась «Стеганография».

Если принять на веру утверждение о том, что «Полиграфия» продолжает темы, развиваемые в «Стеганографии», то следует предположить, что в центре обоих сочинений находится рассмотрение проблем тайнописи. Магический колорит, отличающий «Стеганографию», при этом является лишь внешним прикрытием для рассмотрения криптографических методов. Однако и это заключение не может считаться однозначным.

В течение нескольких столетий со времени написания и распространения текста «Стеганографии» среди читателей и иссле-

дователей идет спор о том, было ли для Тритемия основным магическое или криптографическое содержание прославивших его работ. Одна из этих точек зрения обоснована выше. Вторая предполагает, что третья часть «Стеганографии» является пособием по черной магии, описанием таинственных методов общения людей с духами и т. д.

Последняя версия, подчеркивающая основополагающее значение магии для сочинения Тритемия, зародилась еще до того, как он дописал «Стеганографию». В одном из писем к другу Бостию он поделился мыслями о содержании нового сочинения, которое писал в это время. Адресат не получил письма, поскольку оно прибыло в Гент вскоре после смерти Арнольда Бостия. Однако аббат монастыря не только прочел письмо, но и ознакомил с его содержанием других, в результате Тритемий приобрел славу оккультиста, общающегося с демонами, еще до того, как его «Стеганография» попала в руки к читателям. Возможно, это стало причиной того, что в 1500 г. Тритемий прекратил работу над сочинением, но, как свидетельствует факт написания «Полиграфии», сохранил интерес к вопросам тайнописи, хотя и исключил из своей следующей работы магические пассажи. Итальянский математик Карла Бовилл (1479–1567), который ознакомился со «Стеганографией» Тритемия во время визита к автору, в письме к одному из их общих знакомых, Герману де Ганаю, приближенному французского короля Людовика XII, ставшему впоследствии епископом Орлеана, дает отзыв о сочинении Тритемия. Бовилл был настолько удивлен и даже испуган содержанием труда, наполненного именами духов и подробными описаниями методов их вызывания, что вынужден был через два часа прекратить чтение, опасаясь силы заклинаний, и высказывал предположение, что Тритемий действительно общался с демонами¹⁴. Это письмо было издано в 1510 г. и способствовало поддержанию репутации Тритемия как оккультиста и мага. Безусловно, эту репутацию поддержал и интерес к фигуре самого Тритемия и к его сочинению со стороны таких видных деятелей оккультизма, как Агриппа Неттесгеймский и Джон Ди.

Официальным подтверждением отношения церкви и общественности к «Стеганографии» как к оккультному сочинению явилось включение ее в индекс запрещенных книг¹⁵. За этой работой надолго закрепилась слава одного из основных европейских сочинений по демонологии.

Тритемий пытался открыто возражать. Так, в первой главе третьей части «Стеганографии» он открыто высказывает опасения, что читатели обвинят его в занятиях некромантией и таким обра-

зом итоги написания сочинения не будут соответствовать усилиям, которые автор потратил на его создание. Эти опасения, по словам Тритемия, стали одной из основных причин, по которой «Стеганография» осталась незаконченной.

В предисловии к «Полиграфии» Тритемий также предпринимает попытки защитить свою репутацию и судьбу своей книги. Здесь он поясняет, что в своей работе «Стеганография» обращался не к демонологии, а к так называемой «естественной магии», которая, по его мнению, «чиста, основательна, неизменна и позволена»¹⁶ и не предполагает ничего сомнительного с точки зрения официальной религии. Она базируется на законах природы и не допускает никаких суеверий. «Магия же, если она естественная, приносит не только видимые результаты, но и удивительным образом просвещает разум сведущего в ней человека, а познанием божественного приносит невидимые плоды душе»¹⁷. Но если древние правители и ученые были прекрасно знакомы с ней, то во времена автора занятия ею вызывают осуждение. Отчасти это происходит потому, что те, кто не понимает ее духа, извращают ее сущность. Поэтому «...магия, святая и достойная, которая может быть правильно, чисто и тайно передаваемой авторами, так запутана, обезображена и отравлена, что имя ее, кажется, страшно слышать христианам и для всех оно может быть пугающим и не столько ненавидимым, сколько непроницаемым»¹⁸. Более того, в другом письме Тритемий отмечает, что все то, что было и будет им написано, никак не связано с демонологией и сомнительными с точки зрения христианства магическими заклинаниями и операциями¹⁹.

С начала XVII в. предпринимаются попытки очистить репутацию автора «Стеганографии» от нападок со стороны церковных ортодоксов. Так, два бенедиктинских монаха, братья Карл и Георг Штенгели, и иезуит Адам Таннер пытаются объяснить содержание «Стеганографии» исключительно с точки зрения рассмотрения идей и принципов шифрования. Но они не могли привести четких доказательств правильности своей позиции и к тому же не смогли дешифровать третью книгу труда. Позднее попытки оправдать Тритемия предпринимались неоднократно, например, А. Кирхером, Г. Скоттом, Х. Брайтхауптом и др.

В наше время мнение о том, что «Стеганография» имеет, прежде всего, криптографическое содержание, является наиболее распространенным среди исследователей. В частности, выразителем этой идеи является В. Шумейкер, который указывает, что «Стеганография» посвящена, прежде всего, криптографии, хотя в отношении третьей части это не выглядит очевидным²⁰. Таким образом, не

стоит умалять значение личности и трудов Тритемия в совершенствовании способов шифрования.

При этом основное значение идей Тритемия для развития криптографической мысли связано с его работой, которая получила название «Полиграфия». Тритемий закончил эту работу 28 марта 1508 г. Сочинение состоит из шести книг и содержит посвящение императору Максимилиану I, которому и было лично вручено 26 апреля 1508 г., судя по письмам Тритемия²¹. Издана «Полиграфия» была только после смерти автора, впервые в 1518 г., и выдержала большое количество переизданий. Ее принято считать первым в Европе крупным сочинением, посвященным непосредственно криптографии. Для «Полиграфии», так же как и для «Стеганографии», существовала сокращенная версия из одной части под названием «Ключ к “Полиграфии”» (*Poligraphiae clavis*)²², включающая ряд пояснений к основному труду. Эта версия включалась в некоторые издания «Полиграфии», например, в издание 1613 г.

В начале «Полиграфии» автор определяет цель написания своего сочинения. Она заключалась в том, чтобы рассказать о «конкретных способах тайно писать, с помощью которых короли и властители, знатные и неизвестные, жрецы и простецы, ученые и неученые тайно, безопасно и без всяких сомнений... могли бы обмениваться письмами на расстоянии»²³.

В первых четырех книгах «Полиграфии» приводятся столбцы слов, каждое из которых должно было служить в качестве замены букв в шифруемом тексте. Из таких слов должны были составляться осмысленные фразы, скрывающие сам факт наличия секретного послания. Шестая книга «Полиграфии» содержала обзор известных автору методов шифрования с древних времен до современности с указанием на те из них, которые и в его эпоху разумно использовать на практике.

Пятая часть сочинения содержит созданный Тритемием шифр полиалфавитной замены, ставший известным под названием «Ave Maria». Название его связано с тем, что Тритемий для маскировки тайного письма предлагал применять для замены слова, составляющие фразы с религиозным содержанием. Как было указано выше, в первых двух частях сочинения автор рассматривал систему шифрования, заключающуюся в том, чтобы каждая буква слова заменялась словом из того или иного столбца. Последние содержали слова, относящиеся к различным частям речи в соответствующих грамматических формах, для составления из них осмысленных предложений. В третьей и четвертой части приводились колонки

с наборами букв, где каждая вторая должна была становиться частью секретного послания.

Достоинством такого шифра следует считать возможность составления осмысленных предложений, которые позволяли скрывать тайное сообщение. В качестве недостатка системы шифрования следует указать на то, что при малой длине ключа криптостойкость шифра достаточно низкая, а составление, запоминание и передача длинных ключей связаны с различными трудностями.

Пятая глава «Полиграфии» содержит таблицу замены (“*tabula gesta*”). Изначальный ее алфавит записывался в одну строку, а следующая строка составлялась из предыдущей с помощью сдвига влево.

Далее Тритемий приводил такую таблицу в нескольких формах: алфавит мог записываться в обратном порядке, для шифрования вместо букв применялись цифры и т. п. Важным отличием такого шифра от шифра простой замены являлось то, что после шифрования каждой буквы происходила смена алфавита замены. Таким образом, данный шифр является шифром полиалфавитной замены.

Изобретение Тритемия можно считать независимым открытием, так как не имеется указаний на знакомство автора с работой Лео-на Баттисты Альберти, посвященной криптографии, где впервые в истории западноевропейской мысли приводится описание шифрования методом многоалфавитной замены, выполненное с помощью шифровального диска. Помимо этого, в отличие от трактата Альберти, «Полиграфия» получила больший резонанс среди читающей публики благодаря известности автора и расширившимся к тому времени возможностям книгопечатного дела. Это повлияло на распространение идей криптографии среди широкой общественности, хотя и добавило оккультный оттенок благодаря своеобразной славе Тритемия.

Таким образом, оба сочинения Тритемия, связанные с вопросами тайнописи, внесли значительный вклад в развитие идей криптографии и совершенствование криптографических методов в рассматриваемую эпоху.

«Стеганография» при этом принесла автору больше откликов от современников, чем другая его работа. Это обусловлено тем, что содержание «Стеганографии» отвечало настроениям определенной части интеллектуалов того времени, связанным с интересом к магии, каббале и астрологии, которые так или иначе удавалось сочетать с официальными христианскими доктринами. Привле-

кательной для читателей представлялась и загадочность текстов «Стеганографии». В отличие от нее, «Полиграфия» оказалась лишенной магической составляющей, поскольку после обвинения в использовании средств оккультной магии автор внес коррективы в изначальный замысел работы. В то же время «Полиграфия» вряд ли была обращена и к практикам шифровального дела, таким как, например, дипломаты, использовавшие в тот период хоть и более простые, но более удобные шифры.

Важнейшим остается вопрос о причинах обращения Тритемия к теме тайнописи. С одной стороны, Тритемия интересовали «магические» операции над цифрами и буквами для общения с неземными силами, схожие с теми, которые производились каббалистами с помощью древнееврейского алфавита, что соответствовало духу времени. С другой стороны, Тритемию явно нравилась таинственность и было свойственно тщеславие, заставлявшее его предлагать читателю загадки, над которыми тот порой безуспешно ломал голову.

Однако главной целью обращения Тритемия к криптографии являлось, по всей видимости, то, что она «просвещает разум» и «познанием божественного приносит невидимые плоды душе». Эти слова Тритемий использовал в отношении так называемой «естественной магии», к которой, по всей вероятности, относились для него и занятия тайнописью. При этом его понимание такой естественной магии было не совсем типичным для его времени и предполагало использование заклинаний и процедур, которые многие современники и потомки сочли демонологическими. Стремление защитить себя от таких обвинений привело Тритемия к рассмотрению в «Полиграфии» лишь техник шифрования, в то время как «Стеганография» больше соответствовала замыслу автора. Тем не менее, как отметила немецкая исследовательница работ Тритемия Лиlienфельд, как в «Стеганографии», так и в «Полиграфии» «...сохраняется ощущение связи между техническими приемами шифрования и их пониманием как божественного творения...»²⁴.

Обращение к криптографии Тритемия, в отличие, в частности, от также проникнутой магическим духом тайнописи алхимиков, характеризует именно это внимание к технике шифрования, к занятиям, помогающим проявиться интеллектуальным, в частности математическим, способностям человеческого разума. Это является одной из определяющих отличительных черт западноевропейской криптографии раннего Нового времени по сравнению с эпохой Средних веков.

- ¹ Русецкая И.А. История криптографии в Западной Европе в раннее новое время. СПб.: Центр гуманит. инициатив; Университетская книга. СПб., 2014.
- ² Reich H. Der Index der verbotenen Bücher, ein Beitrag zur Kirchen- und Literaturgeschichte. Vol. 2. Bonn, 1885. S. 183.
- ³ Schneegans W. Abt Johannes Trithemius und Kloster Sponheim. Kreuznach, 1882. S. 185.
- ⁴ Arnold K. Johannes Trithemius (1462–1516). Zweite, bibliographisch und überlieferungsgeschichtlich neu bearbeitete Auflage. Würzburg, 1991. S. 253–254.
- ⁵ Vigenere, Blaise de. Traicte des chiffres. Paris, 1586. P. 13, 182.
- ⁶ Trithemius J. Steganographia: Hoc est: Ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa; authore referendissimo et clarissimoviro, Joanne Trithemii Abbatis Spanheimensis... Francofurti: Matthias Becker, 1606.
- ⁷ Heidel W.E. Joannis Trithemii Steganographia. Moguntiae: Joannes Petrus Zubrodt, 1676.
- ⁸ Gustavi Seleni Cryptomenytices et cryptographia libri IX. Lüneburg: Johannes & Henricus Stern, 1624.
- ⁹ Ernst T. The numerical-astrological ciphers in the third book of Trithemius's Steganographia // Cryptologia. 1998. Vol. 22. N. 4.
- ¹⁰ Ibid. P. 327.
- ¹¹ Ibid. P. 330.
- ¹² Ibid. P. 337.
- ¹³ Schneegans W. Abt Johannes Trithemius und Kloster Sponheim. Kreuznach, 1882. S. 200.
- ¹⁴ Ibid. P. 190–191.
- ¹⁵ Reusch H. Op. cit. S. 183.
- ¹⁶ Joannes Trithemius ad Joachimum Marchionem Brandenburgensem, de rebus convenientibus vero Mago // Trithemius J. Joannis Trithemii... Libri poligraphiae VI. [Strassburg], 1613. P. 49.
- ¹⁷ Ibid. P. 51.
- ¹⁸ Ibid. P. 53.
- ¹⁹ Ibid. P. 102–103.
- ²⁰ Shumaker W. Renaissance Curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language. N. Y., 1982 (Medieval and Renaissance Texts and Studies. Vol. 8).
- ²¹ Schneegans. Op. cit. P. 197.
- ²² Clavis Polygraphiae Joannis Tritemii... Basel: Joannes Haselberg, 1518.
- ²³ Trithemius J. Joannis Trithemii Libri poligraphiae VI. [Strassburg], 1613. P. 44.
- ²⁴ Лилиенфельд Ф. Иоанн Тритемий и Федор Курицын (о некоторых чертах раннего Ренессанса на Руси и в Германии) // Культурное наследие Древней Руси. М., 1976. С. 120.