С. В. Запечников

ИЗ ИСТОРИИ КРИПТОГРАФИИ: ТАЙНОПИСЬ И ТАЙНЫЕ КОММУНИКАЦИИ В АНТИЧНОМ МИРЕ

Введение

Хорошо известно, что криптография относится к древнейшим отраслям человеческой деятельности. Однако вплоть до конца XIX в. продолжался донаучный этап развития криптографии, когда она была скорее ремеслом или даже искусством, доступным лишь избранным лицам, умевшим делать тексты непонятными для непосвященных. Вместе с тем в течение этого длительного периода копились те методы и факты, которые легли в основу современной, научной криптографии, а также криптоанализа.

К сожалению, в многочисленных современных учебниках и справочниках ранним этапам истории криптографии не уделяется должного внимания. Разрозненные факты, упоминаемые в литературе, в лучшем случае служат лишь «фоном», который, хотя и демонстрирует в учебных целях базовые принципы шифрования, но неизменно служит для того, чтобы «оттенить» примитивность донаучных методов криптографии по сравнению с современными.

По мнению автора, сравнение донаучных приемов защиты письменных текстов, тем более ранних, появившихся много веков и даже несколько тысячелетий назад, с нынешними алгоритмическими методами, опирающимися на строгую логику и установленные многими поколениями математиков закономерности, вряд ли корректно. Как было показано в предыдущих публикациях автора, таких как [1], древнюю тайнопись следует считать феноменом, относящимся к сфере языкового сознания определенной части носителей естественного человеческого языка. Владение авторов тайнописных текстов какими-либо изощренными методами формальной логики, а тем более сколько-нибудь адекватным решаемым задачам математическим аппаратом ни в одном из сохранившихся свидетельств не зафиксировано. Именно с этих позиций, как комплексное явление, охватывающее и собственно язык (от графики до синтаксиса), и литературу (своеобразные жанры, характерные для «тайных» текстов), — будет рассматриваться тайнопись далее.

В настоящей статье предпринимается попытка охватить наиболее ранний, но и наиболее длительный по времени период развития тайнописи: с древнейших времен, в которые было зафиксировано ее существование, и до конца периода Древней истории (по общепринятой классификации — до падения Западной Римской империи в 476 г. н. э.). Основным же рассматриваемым периодом как по количеству накопленных фактов, так и по значимости будет греко-римская древность, то есть античный мир.

1. Источники по истории античной тайнописи

При незначительном числе сохранившихся первоисточников литература по истории криптографии античного периода в наше время довольно обширна.

В настоящем исследовании использовались переведенные на русский язык сочинения античных авторов: «История» Геродота (ок. 484 — 425 г. до н. э.) [2], «О перенесении осад» Энея Тактика (IV в. до н. э.) [3], «Всеобщая история» Полибия (ок. 201 — ок. 120 г. до н. э.) [4], «Жизнеописания» Плутарха (ок. 45 — ок. 127 г. н. э.) [5], «Жизнь двенадцати цезарей» Гая Светония Транквилла (ок. 70 — ок. 122 г. н. э.) [6].

В XX в. история криптографии по преимуществу рассматривалась изолированно представителями двух совершенно разных предметных областей: историками и специалистами по защите информации. Это определило большую разницу в методологии исследований и вместе с тем их изолированность и нередко односторонность. Из работ наших современников наибольший интерес представляют масштабные исследования историков [7, 8] и криптографов [9, 10]. Из работ,

вышедших в самое последнее время, особенно ценными выглядят исследования отечественного историка И. А. Русецкой [11] и американского историка науки Крэга Байера [12]. В работе [11] осуществлен глубокий анализ развития криптографии в Западной Европе в раннее Новое время (XV–XVII в.); криптография в античном мире рассматривается в ней с целью поиска истоков и раскрытия закономерностей становления западноевропейской криптографии в Новое время. Работа [12] охватывает широкий временной диапазон с древнейших времен до нашего времени; анализ античных шифров проводится в ней наряду со многими другими шифрами, причем дается, хотя и в ограниченной форме, анализ математических свойств этих шифров с позиций современной науки. Гораздо более солидные части, посвященные математическому анализу свойств античных шифров, имеют книги [10] и [13].

Чтобы верно позиционировать объект нашего рассмотрения относительно более поздних и более «зрелых» методов криптографической защиты информации, таких как ручные шифры, мы предпочли бы определить античную тайнопись как протокриптографические приемы преобразования текстов, используя приставку *прото-* (от греч. protos — «первый»), указывающую на первичность, зачаточность данного явления как истока, начала, предвестия научной криптографии.

2. Функции тайнописи в античном мире

Разрешение вопроса о предпосылках зарождения тайнописи, выявление и анализ функций тайнописи в человеческом обществе на ранних этапах ее становления — не такие простые задачи, как может показаться на первый взгляд. Для полного ответа на эти вопросы потребовалось бы решить сверхзадачу — понять психологию, проникнуть в глубь сознания, восстановить ход мысли людей, живших тысячелетия назад. Вот что пишет о недостижимости этой цели академик Б. В. Раушенбах: «В детстве у меня было две мечты, очень меня увлекавшие: Древний Египет и Космос. Я выбрал Космос, потому что это было реально, а Древний Египет — нереально… Почему Египет и Космос? Может быть, потому, что и то, и другое недостижимо — раскопки, углубление в забытые пласты Земли и полет человека к звездным мирам?» [14, с. 113].

Исследование функций тайнописи обычно являлось прерогативой историков. Отношение криптографов к этому вопросу, как представляется, всегда было довольно прямолинейным: для чего же еще может служить тайнопись, как не для сохранения конфиденциальности текстов? Однако, как это ни парадоксально, но на основе анализа всего массива работ, посвященных истории античной «протокриптографии», приходится предполагать, что как раз функция сохранения конфиденциальности посланий не всегда была главной в древних обществах, а иногда выполнения этой функции и вовсе не требовалось от тайнописи!

Двоякая роль тайнописи в древних обществах весьма точно подмечена в работе И. А. Русецкой: «Задачи, стоявшие перед криптографией, можно разделить на два типа. Первый тип связан с использованием криптографии в религиозной, оккультной, магической и другой подобной практике с целью скрыть некоторые сведения и знания от непосвященных. Криптография в этом случае может восприниматься как магическое искусство. Второй тип задач связан с реализацией практических потребностей передачи информации, содержащей секретные сведения. Применение криптографических методов лишено при этом мистической окраски, они используются в борьбе за политическое, военное, экономическое господство» [11, с. 6]. Нельзя не согласиться именно с такой расстановкой приоритетов: вероятно, истоки появления тайнописи следует искать именно в необходимости сакрализации слов, понятий, имен, явлений и целых текстов. Автор работы [11] указывает на то, что одна из самых состоятельных версий происхождения этого явления принадлежит Дж. Фрэзеру. Действительно, в книге [15] предлагается весьма убедительное обоснование того, что тайна имени, тайна слова и связанные с ней табу есть общий закон первобытного мышления, «в сферу действия которого попадают простые смертные, боги, цари и жрецы».

С распространением письменности, позволившей сделать слово долговечным, существовавшие в устной речи табу стали переноситься на письмо, что и привело к зарождению простейших форм тайнописи одновременно или почти одновременно с письменностью. Значит, «тайный язык» так же первичен по отношению к тайнописи, как естественная человеческая речь — по отношению к письменности. Тот факт, что тайнопись обнаруживается среди древнейших известных образцов письма (как будет отмечено в п. 3), свидетельствует в пользу этой гипотезы.

Лишь позднее у различных социальных групп, владевших грамотой: правителей государств, военачальников и их приближенных, обладавших уникальными знаниями мастеров — наступает осознание того, что некие сведения (знания, имена, количества) при помощи тайнописи можно защитить не только от сверхъестественных сил: колдовства, злых духов, черной магии и др. — но и от иноплеменников или от незаслуживающего доверия окружения. Процитируем еще один тезис из работы И. А. Русецкой, хотя и высказанный в другом контексте, по в данном случае достаточно точно отражающий суть явления: «Однако были необходимы определенные условия, которые смогли сделать возможным переход от признания значения связи между начертанием, а также комбинациями букв к возможности скрытия с их помощью определенных знаний и осуществлению в том или ином виде криптографических операций, которые могли составлять внешнюю сторону этого процесса» [11, с. 80].

Таким образом, есть основания предполагать, что практические, социальные функции криптографии исторически все же были вторичными, а ход мысли древних следовал схеме: от «магического» *содержания* речи, произнесенной на «тайном языке», к тайнописной *форме* текста и от него уже — к «практическому» *содержанию* сведений, закодированных тайнописью, и социальным аспектам их *использования*.

Обе функции тайнописи: «магическая» и «практическая» — тесно связаны с *тайными коммуникациями* (в широком смысле слова): только в первом случае речь идет о коммуникациях со сверхъестественными силами, а во втором — о коммуникациях внутри человеческого общества. Вместе с тем важно отметить, что тайные коммуникации (как в пространстве, так и во времени) могут осуществляться не только посредством тайнописи — во все исторические эпохи параллельно с криптографией развивались приемы стеганографии, всевозможные способы физической защиты сообщений, их кодирование и различные комбинации перечисленных приемов.

3. Древнейшие образцы тайнописи Египта, Индии и Ближнего Востока

О древнейших приемах тайнописи известно очень немногое: от периода ранее V в. до н. э. сохранились лишь обрывочные, зачастую ненадежные свидетельства ее существования. Два самых известных в наши дни материальных свидетельства тайнописи иллюстрируют обе основные функции тайнописи: «магическую» и «практическую».

Самое старшее по возрасту из известных свидетельств существования тайнописи, сохранившихся до наших дней, — вырезанная на камне «магическая» надпись в египетской местности Бени-Хасан на гробнице знатного вельможи Хнумхотепа, состоявшего на службе у фараона Аменемхета II и ответственного за постройку ряда монументальных сооружений [8, с. 4–5]. Надпись относится приблизительно к 1900 г. до н. э. Эта надпись была сделана не обычными, а видоизмененными иероглифами, тем не менее она все равно читается без знания каких-либо специальных ключей. По мнению египтологов, этот прием отнюдь не имел целью засекретить содержание текста от посторонних, но нужен был для придания торжественности, особой значимости тексту, а с точки зрения древних египтян с их непоколебимой верой в загробную жизнь — для привлечения к умершему внимания потусторонних сил.

Египтологам известен целый ряд других подобных надписей, относящихся к более позднему времени, в частности надписи на саркофагах фараона Сети I, запись гимна в честь бога Тота. Все надписи

похожи друг на друга в том, что нанесены видоизмененными иероглифами, а нередко дублируются в обычной форме рядом с измененной. Такое письмо строилось по принципу ребуса, по всей видимости, с целью привлечь внимание читателей, заставить их задуматься и вызвать желание разгадать смысл написанного, тем самым выразив почтение умершему. По выражению Д. Кана, «добавление элемента секретности в преобразование иероглифов породило криптографию. Правда, это напоминало скорее игру, поскольку преследовалась цель задержать разгадку только на самое короткое время. Поэтому криптоанализ также заключался всего лишь в раскрытии головоломки. Таким образом, древнеегипетский криптоанализ был квазинаукой, в отличие от этой современной, чрезвычайно серьезной области научных знаний. Однако всем великим делам свойственны скромные начинания. Иероглифы Древнего Египта действительно включали, хотя и в несовершенной форме, два элемента — секретность и преобразование письма, которые составляют основные атрибуты криптографии» [8, с. 12—13].

Второе древнейшее свидетельство протокриптографии — месопотамская глиняная табличка с нанесенной на нее клинописью, найденная археологами в середине XIX в. при раскопках библиотеки царя Ашшурбанипала близ берега реки Тигр на территории современного Ирака: это представитель «практического» направления древнейшей тайнописи. Она относится приблизительно к 1500 г. до н. э. Надпись на табличке была выполнена «нестандартной», измененной клинописью: после дешифровки оказалось, что на ней записан рецепт глазури для покрытия керамических изделий. Вероятно, дворцовый мастер, который изобрел рецепт глазури, записал его для памяти, но таким образом, чтобы он не был понятен другим людям, в руки которых попала бы эта табличка. В табличках, относящихся к более позднему времени, подобные сведения уже не были зашифрованы: видимо, с течением времени рецепт стал известен всем, и скрывать его уже не было необходимости.

Есть косвенные свидетельства того, что протокриптографические приемы были известны цивилизациям Индии и восточного Средиземноморья. Так, в [8] есть ссылки на два древнеиндийских трактата: «Артасастру» и «Камасутру». В первом, посвященном вопросам политики и управления государством, есть рекомендация, чтобы глава шпионской службы государства давал указания своим агентам «тайным языком», в иносказательной форме. Во втором среди 64 искусств Сарасвати, которыми должна овладеть женщина, упоминаются умение читать между строк, понимать смысл зашифрованного текста, а также умение говорить, меняя форму слова, например, вставляя между соседними слогами лишнюю букву [16, с. 18]. Однако прямых доказательств использования тайнописи в Индии не сохранилось.

Простейшие приемы использования криптографии, известные под названием «атбаш», встречаются в священных иудейских книгах. Атбаш — это способ замены букв древнееврейского алфавита по принципу замещения в тексте каждой i-й по порядку следования в алфавите буквы на $(n-i+1)$-ю, где n — общее число букв в алфавите, то есть составление такой таблицы замены, в которой алфавит шифртекста есть записанный в обратном порядке алфавит открытого текста. Этот способ тайнописи был, по всей видимости, изобретен иудейской сектой Евсеев и использовался для написания различных имен и названий, чтобы избежать преследований. Подобная тайнопись с «переворачиванием» алфавита использовалась в дальнейшем различными тайными обществами и группами в разных странах. Но первые известные примеры ее применения, как считается, содержатся в библейской Книге пророка Иеремии: «И всех царей севера, близких друг к другу и дальних, и все царства земные, которые — на лице земли, а царь Сесаха выпьет после них» (Иер 25: 26) и «Как взят Сесах и завоевана слава всей земли!» (Иер 51: 41). Как доказано исследователями Библии, непонятное слово «Сесах» здесь — это атбаш древнееврейского слова «Бабель», означавшего Вавилон. Д. Кан также упоминает еще один эпизод из Библии, когда внезапно возникшая кисть руки пишет на стене загадочные слова, которые не смогли понять вавилонские мудрецы, но объяснил пророк Даниил (Дан 5: 24—29). Вряд ли этот эпизод можно считать прямым доказательством

существования тайнописи, но он хорошо демонстрирует характерный прием изложения важного содержания в форме своеобразных загадок, ребусов, намеков и т. п., заставляющих читателя задуматься, обратить внимание на подчеркнуто торжественный стиль изложения, проявить творческий подход к интерпретации текста. Имеются также предположения, что атбаш использован для преобразования отдельных слов и фраз в Кумранских рукописях.

Попутно заметим, что вокруг древнейших литературных памятников (древнеегипетских папирусов, библейских книг, древнеиндийских трактатов) существовало и существует множество спекуляций о якобы «зашифрованных» в них тайных знаниях погибших цивилизаций. Никакого отношения к подлинно научному изучению истоков криптографии они не имеют. Убедительно доказанных фактов присутствия тайнописи в древних текстах не так много, и они свидетельствуют о применении лишь простейших форм тайнописи.

На основании анализа изложенных здесь фактов можно заключить, что протокриптографические приемы преобразования текстов в целом характеризуются тем, что в них используются те же технические приемы, что и в более поздних методах, таких как «ручные» шифры, — это разные способы замены исходных символов на иные символы. Делается это с разнообразными целями, среди которых, однако, цель обеспечения секретности текста явно не выявляется.

4. Проблемы идентификации тайнописи в древнейших письменных памятниках

Определению точного времени, к которому относится появление первых тайнописных текстов, а таким образом, и «возраста» криптографии как науки мешает наличие целого массива не поддающихся дешифровке текстов на различных материальных носителях, найденных в разное время археологами. Дешифровка забытых языков — это отдельная, весьма проблематичная область научных исследований. Ей посвящена обширная литература, мы же лишь вскользь коснемся ее в той мере, в какой она представляет интерес для истории криптографии.

Пожалуй, самым известным и самым ярким представителем этой группы памятников является Фестский диск, найденный итальянскими археологами 3 июля 1908 г. при раскопках дворцового комплекса в древнем городе Фест на о. Крит и ныне хранящийся в археологическом музее греческого Ираклиона. Фестскому диску посвящена обширная литература: из работ на русском языке в первую очередь заслуживают упоминания книги [17] и [18]. С момента открытия Фестский диск привлек к себе огромное внимание из-за уникального письма, которым нанесена надпись с двух сторон глиняного диска. Исследования, продолжающиеся с начала XX в., позволили найти более или менее состоятельные ответы на часть вопросов, касающихся направления письма, системы письма, предполагаемого содержания сообщения. Однако большинство полученных ответов до сих пор остаются дискуссионными. За долгие годы Фестский диск стал своего рода символом для всех интересующихся историей древних цивилизаций. На момент обнаружения письменность диска коренным образом отличалась от всех известных письменностей. Но впоследствии в разное время и в разных местах был обнаружен еще целый ряд памятников с письменами, в той или иной степени родственными знакам на Фестском диске: надпись на бронзовой секире из Аркалохори, каменный алтарь из Мальи, священный диск из Мальяно и др. По состоянию на начало XXI в. недешифрованными остаются также древнейшие рисуночные прототипы знаков шумерской клинописи (называемые протошумерским письмом) и протоэламское письмо, которое, возможно, не имеет отношения к шумерской клинописи, протосинайское письмо, библское письмо, древнеханаанейское письмо, ронго-ронго (письменность острова Пасхи) и целый ряд других [19].

Сходство задачи прочтения забытых письменностей с задачей дешифрования, стоящей перед криптоаналитиком, очевидно. Именно поэтому в среде «любителей древности» обе задачи нередко смешиваются или вообще отождествляются. Тем не менее разница между ними весьма существенна. При попытке прочтения древних письменностей исследователь имеет дело с такой системой письма,

для которой с большой долей вероятности не ставилась задача сокрытия каких-либо сведений от своих современников, владевших грамотой. Мы не понимаем содержание написанного из-за того, что древняя система письма кардинально отличалась от всех используемых в настоящее время. И это различие порождено не чьим-то умыслом, направленным на сокрытие или осложнение раскрытия письменно зафиксированных сведений, а очень существенными ментальными и психологическими различиями между представителями древней и современной нам цивилизаций. Как только появляются достаточные условия, надежная опора для прочтения древнего текста, он становится читаемым, лишаясь мнимой «секретности». Классический пример — это история прочтения египетского иероглифического письма французским ученым Ж.-Ф. Шампольоном на основе текстов Розеттского камня, содержавшего надписи идентичного содержания на трех языках, в том числе на неизвестном древнеегипетском и известном древнегреческом. Другой пример — история прочтения древнего письма майя, в чем очень существенная роль принадлежит советским ученым Ю. В. Кнорозову и Т. А. Проскуряковой. Иное дело — криптоанализ: здесь исследователь имеет дело с такой (научной) системой шифрования или (донаучной) системой тайнописи, изначальная и главная цель которой — разрушение семантики текста для непосвященного с сохранением возможности восстановления его смысла для посвященного в секреты тайнописи (или знающего ключи шифрования), а в идеале — разрушение всякой «опоры», которой мог бы воспользоваться криптоаналитик (что было достигнуто только в начале XX в. с изобретением совершенно секретного шифра).

Как отмечалось выше, тайнопись по своему происхождению была не чем иным, как письменностью некоторого «тайного языка» общения со сверхъестественными силами или «тайного языка» общения между собой определенных классов древнего общества. Такие «тайные языки», однако, нельзя ставить в один ряд с естественными языками, функционирующими в человеческом обществе. «Тайный язык» может иметь свою систему письма, он может иметь и свою специфическую лексику, но ни один «тайный язык» не имеет своей собственной грамматики и синтаксиса. Как правило, грамматика и синтаксис такого языка либо элементарны, либо заимствуются без изменений из того естественного человеческого языка, надстройкой над которым он является. Разумеется, «тайный язык» может быть и бесписьменным — в современном мире это, например, жаргоны различных узких социальных групп или субкультур, но бесписьменные языки не представляет интереса в контексте обсуждения криптографии. Если же письменность у «тайного языка» имеется, то эта тайнопись является просто иной, альтернативной формой представления того же содержания на материальном носителе.

В этом смысле для расшифровки забытых письменностей всегда имеется больше «зацепок», больше возможностей провести аналогии, применить интуицию, опереться на гипотезы историков, культурологов, филологов, лингвистов. Проблема их прочтения шире и многограннее, чем задача раскрытия шифртекста криптоаналитиком, хотя чисто технически работа криптоаналитика может быть более трудоемкой. Однако для истории криптографии основная проблема, связанная с этими памятниками, касается даже не их прочтения как такового, а того, чем окажется прочитанный текст. Это может быть текст на еще неизвестном современной науке забытом древнем языке, либо неизвестная система тайнописи для известного древнего языка (что было бы проще всего, но маловероятно), либо неизвестная система тайнописи для неизвестного языка, либо вообще надпись нетекстового характера (например, существует гипотеза о календарном характере Фестского диска). Таким образом, прочтение древнейших памятников письма способно принести новый материал для историков криптографии и привести как к переоценке «возраста» криптографии и длительности отдельных этапов ее развития, так и к открытию новых приемов преобразования текстов, использовавшихся древними цивилизациями. Кроме того, время от времени археологам удается обнаруживать новые письменные памятники далекого прошлого. В этом смысле криптография по-прежнему остается наукой «с непредсказуемым прошлым».

5. Тайнопись и тайные коммуникации в Древней Греции

В современной просветительской и учебной литературе сложилась традиция рассматривать в качестве важнейших примеров классических шифров, происхождение которых относят к периоду Древней Греции, три типа шифров: 1) так называемую скиталу (другое название — сциталь); 2) диск Энея, линейку Энея и книжный шифр Энея; 3) квадрат Полибия.

Однако внимательное ознакомление с результатами исследований историков убеждает в том, что традиционное изложение этих способов шифрования во многом носит легендарный характер. Широко тиражируемые в литературе версии этих шифров представляют собой неоправданные модернизации тех приемов преобразования текстов, которые использовались древними греками, а нередко утвердительно называются шифрами те способы преобразования текстов, возможность использования которых греками для обеспечения секретности каких-либо сведений весьма дискуссионна.

Самый известный из всех древнегреческих шифров — *скитала* — шифровальное устройство в виде длинной деревянной палки с наматываемой на него полоской папируса, ремнем или иным материалом для письма. В наше время скитала стала своеобразным символом и даже принята в качестве эмблемы Американской криптографической ассоциации (American Cryptogram Association). По наиболее распространенной версии, берущей свое начало из «Сравнительных жизнеописаний» древнегреческого историка Плутарха, это шифровальное устройство использовалось в Спарте, в частности, знаменитым лакедемонянским полководцем Лисандром: «Лисандру послали скиталу с требованием вернуться. А скитала вот что такое. Отправляя к месту службы начальника флота или сухопутного войска, эфоры берут две круглые палки совершенно одинаковой длины и толщины. Одну они оставляют себе, другую передают отъезжающему. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, наматывают ее на свою скиталу, не оставляя на ней ни одного промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, они пишут на нем то, что нужно, а написав, снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, но разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, располагая ее извивы в прежнем порядке, чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение. Полоса папируса называется, как и деревянная палка, “скиталой”...» [5].

Скитала осуществляет перестановку символов, и если она действительно использовалась для целей шифрования, то является шифром простой замены. Считается также, что Аристотелем (384–322 г. до н. э.) был предложен способ раскрытия текстов, зашифрованных при помощи скиталы: для этого следует наматывать полоску с шифртекстом на конус с медленно изменяющимся диаметром до тех пор, пока на нем не обнаружится такой участок, где между витками ленточки читается фрагмент осмысленного текста. Однако автору настоящей статьи пока не удалось обнаружить, из какого первоисточника идет традиция приписывать Аристотелю эту заслугу.

И. А. Русецкой проведено тщательное исследование сочинений древних авторов, в которых упоминается скитала (Архилоха, Пиндара, Фукидида, Ксенофонта, Диодора Сицилийского) [11], откуда довольно убедительно следует, что ни один другой первоисточник, кроме Плутарха, не говорит прямо о применении скиталы в качестве шифровального устройства. Но время жизни самого Плутарха отделено от времени жизни Лисандра примерно пятью веками, так что весьма вероятно, что Плутарх записал уже сформировавшуюся к тому времени и передававшуюся в устной традиции легенду о скитале. «Приведенные свидетельства греческих историков позволяют убедиться в том, что основные значения слова “скитала” не предполагали, что она рассматривалась как устройство для шифрования. Конкретные примеры ее использования могли быть различными. При этом основным назначением скиталы можно считать применение ее для удобства доставки или хранения посланий,

наматываемых на палочку. Эта версия может быть косвенно подтверждена и исследованиями истории и культуры Спарты. Известно, какими знаниями и умениями обладали спартанцы в вопросах подготовки воинов и осуществлении военных мероприятий. Но развитие этого общества не было отмечено большими достижениями в области культуры, образования и письменности. В этих условиях маловероятным представляется изобретение спартанцами шифровального устройства» [11, с. 47].

Вместе с тем очевидно, что представление о принципиальной возможности использования скиталы как шифровального устройства возникло уже в древности, но применялась ли она на практике по этому назначению, на текущий момент достоверно установить не удается.

Другая известная «серия» шифровальных приспособлений связана с именем Энея Тактика (IV в. до н. э.) — греческого полководца, единственный сохранившийся до нашего времени трактат которого — «О перенесении осад» [3].

Первый описанный в нем шифровальный инструмент известен как *диск Энея* — это небольшой диск с проделанными в нем вдоль периметра отверстиями, число которых равно числу букв в алфавите. Через отверстия должна была последовательно протягиваться нить соответственно буквам шифруемого текста. В итоге диск с опутанной вокруг него нитью и будет служить шифртекстом, а ключом к нему является соответствие между отверстиями и буквами.

Похожее устройство, но в виде линейки с засечками, соответствующими буквам, получило название *линейки Энея*. В отличие от предыдущего случая, здесь в качестве шифртекста достаточно передать только нить с завязанными на ней в местах прохождения через прорези узелками. Оба устройства — это шифры простой замены.

Наконец, так называемый *книжный шифр Энея* — это способ передачи информации при помощи малозаметных пометок возле букв в тексте книги: дырочек, точек и т. п. По существу это не шифр, а прием стеганографии. Описанные Энеем приемы шифрования, безусловно, возможны, но выглядят несколько искусственными или даже непрактичными. К тому же никакой другой литературный источник не упоминает фактов применения этих устройств на практике [11, с. 43].

Третий широко известный древнегреческий прием шифрования — так называемый *квадрат Полибия* — тоже не что иное, как шифр простой замены. Свое название он получил потому, что описан во «Всеобщей истории» Полибия.

«Нужно взять все буквы азбуки в последовательном порядке и разделить их на пять частей по пяти букв в каждой части. Хотя в последней группе одной буквы и не достанет, но это не мешает. Затем обе стороны, желающие сноситься между собою посредством сигнальных огней, изготовляют себе по пяти досок и на каждую доску наносят одну из групп букв по порядку, потом условливаются между собою, так что та сторона, которая должна подавать весть, поднимает факелы первая, притом два факела разом, и не опускает их до тех пор, пока не ответит другая сторона. Делается это ради уведомления друг друга с помощью сигнальных огней, что все готово. Когда факелы убраны, сторона, подающая весть, поднимает новые факелы с левой стороны, с целью указать, которую из досок следует смотреть, именно: один факел, если первую доску, два, если вторую, и так далее. Точно таким же способом поднимаются другие факелы с правой стороны, чтобы дать понять, какую из букв, находящихся на доске, должно написать тому, кто получает знак.

Когда соглашение состоялось и стороны разошлись по своим местам, каждая из них должна иметь при себе зрительный прибор с двумя отверстиями, дабы получающий известие мог видеть через одно отверстие правую сторону, через другое левую. Подле зрительного прибора в землю вколачиваются стоймя доски, причем как с правой, так и с левой стороны нужно оградить себя забором в десять футов длины и в рост человека вышины: благодаря этому ясно различаются факелы, когда они подняты, и совсем прячутся, когда убраны… Когда слова начертаны на дощечке, производится затем передача их с помощью факелов: первая буква начертания К; находится она во

втором разряде и на второй доске. Поднять нужно два факела с левой стороны, тогда получающий весть знает, что ему нужно посмотреть вторую дощечку; потом с правой стороны поднимается пять факелов, которые и означают букву К, пятую во втором разряде, и тот, кто получает весть, должен начертать ее на дощечке. Затем поднимаются четыре факела с левой стороны, так как буква Р принадлежит к четвертому разряду, далее два с правой, потому что это — вторая буква четвертого разряда. После это принимающий известие пишет букву Р, и так далее в том же порядке. При таком способе каждое происшествие сообщается в точности» [4, с. 148—149].

Описанный Полибием способ расположения букв греческого алфавита в виде квадратной таблицы и кодирования каждой буквы двумя числами — номером строки и столбца таблицы, в которых она расположена, — вообще говоря, тоже не может считаться шифром. Этот код (в некотором смысле — прообраз всем известной телеграфной азбуки Морзе) предназначен для ускорения передачи сообщений, особенно в условиях местности со сложным рельефом: свет факелов виден издалека и позволяет передать не очень длинное сообщение быстрее и с меньшими затратами сил, чем его смог бы довезти посыльный. Шифром он станет только тогда, когда в нем будет предусмотрена возможность выбора и смены ключей, то есть в данном случае — смены самой таблицы соответствия букв и пар чисел. Но именно об этом-то в сочинении Полибия нет ни слова!

Таким образом, в отношении всех трех рассматриваемых приемов преобразования текстов нет достаточных оснований утверждать (как это принято в большинстве современных литературных источников), что они являются первыми известными «ручными» шифрами перестановки и замены. Таковыми их желают видеть современные криптографы, но таковыми не осознавали их сами древние греки.

Геродот в своей «Истории» также упоминает два примененных греками приема, бесспорно относящихся к стеганографии.

Вот первый рассказ про голову раба: «А как раз в это время прибыл к Аристагору из Сус вестник от Гистиея (на голове у вестника были написаны письмена) с советом отложиться от царя. Ведь Гистией желал склонить Аристагора к восстанию, но не мог найти другого безопасного способа [передать свой совет], так как все дороги [из Сус] охранялись. Тогда Гистией велел обрить голову своему верному слуге, наколол на голове татуировкой знаки, а затем, подождав, пока волосы отрастут, отослал его в Милет. Гистией дал слуге только одно поручение: прибыв в Милет, просить Аристагора обрить ему волосы и осмотреть голову. Знаки же на голове слуги, как я уже сказал, призывали к восстанию» [2, кн. 5: 35].

И вот второй, не менее известный, про восковую табличку: «Взяв двухстороннюю дощечку [для письма], он (Демарат. — *С. З.*) соскоблил с нее воск. Затем на дереве дощечки написал замысел царя и снова залил воском написанное, чтобы чистая дощечка не могла возбудить подозрения у дорожных стражей. Когда же дощечку доставили в Лакедемон, то лакедемоняне не могли понять, [что это значит]. Наконец, как мне рассказывали, дочь Клеомена, супруга Леонида, Горго разгадала смысл [посылки]. Она сказала, что нужно соскоблить воск и тогда на дереве обнаружатся буквы. Лакедемоняне так и сделали, нашли надпись прочитав ее, отослали остальным эллинам. Так, по рассказам, распространилась весть [о походе]» [2, кн. 7: 239]. Таким образом, приемы тайных коммуникаций в Древней Греции, как и предполагаемые шифры, были основаны, главным образом, на эвристических соображениях и смекалке.

В завершение этого раздела сделаем еще одно немаловажное примечание: несмотря на то что слово «криптография» греческого происхождения (от др.-греч. κρυπτός — «тайный, скрытый» + γραφω — «пишу»), в языке древних греков его не было — оно стало употребляться позднее, лишь в византийский период. Для характеристики тайнописи использовались самые разные понятия, но только не слово «криптография». Это свидетельствует в пользу того, что

древние греки не осознавали все то, что в наше время принято относить к сфере криптографии (и тем более криптоанализа), как целостное и системное явление. Их способы защиты сообщений были приемами «на случай».

Как представляется, сделанные здесь выводы нисколько не умаляют достоинства криптографии как одной из самых древних отраслей человеческой деятельности и фундаментальных отраслей знания. Напротив, они, с одной стороны, позволяют в некотором роде приблизиться к установлению исторической справедливости и избавиться от широко распространенных заблуждений и мифов, а с другой стороны, обогащают историю науки, демонстрируя сложность и неоднозначность путей развития криптография и силу человеческого разума, который, несмотря на многочисленные сложности практической постановки задач и выбора методов их решения, в конечном счете сумел отыскать оптимальные способы криптографической защиты информации среди большого множества альтернатив и вариантов.

6. Тайнопись и тайные коммуникации в Древнем Риме

Не менее, чем древнегреческие протокриптографические приемы, известен использовавшийся в Древнем Риме шифр, связанный с именем Гая Юлия Цезаря. Он описан римским писателем и историком Светонием: «Существуют и его письма к Цицерону и письма к близким о домашних делах: в них, если нужно было сообщить что-нибудь негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не складывалось ни одного слова. Чтобы разобрать и прочитать их, нужно читать всякий раз четвертую букву вместо первой, например, D вместо A и так далее» [6, с. 27].

Это еще один классический пример шифра простой замены для латинского алфавита с циклическим сдвигом букв в алфавите шифртекста на 3 позиции влево относительно алфавита открытого текста. По свидетельству того же автора, похожим шифром, только со сдвигом на 1 позицию влево, пользовался император Август: «Орфографию, то есть правила и предписания, установленные грамматиками, он не старался соблюдать и, по-видимому, разделял мнение тех, кто думает, что писать надо так, как говорят... Когда он пользуется тайнописью, то пишет B вместо A, C вместо B и так далее таким же образом, а вместо X ставит двойное A» [6, с. 71].

В этих случаях источники прямо упоминают об использовании методов преобразования текстов для того, чтобы сделать их непонятными для непосвященных, то есть здесь мы, бесспорно, имеем дело с сознательным использованием шифров. Помимо двух упомянутых вариантов шифра, римлянам были известны и приемы стеганографии: «письмо намеками», намеренно неясное письмо, пересылка писем в ножнах меча и т. п. (см. [11, с. 49–50]). Также в Древнем Риме была изобретена скоропись, известная под названием «тиронское письмо». Ее изобретение приписывается Тирону — секретарю Цицерона. Ныне способ письма посредством системы особых знаков и сокращений, дающих возможность быстро записывать устную речь, известен под названием стенографии (от др.-греч. $\sigma\tau\varepsilon\nu\circ\varsigma$ — «узкий, тесный» + $\gamma\rho\bar{\alpha}\phi\,\omega$ — «пишу»).

Таким образом, не остается сомнений, что в Древнем Риме были известны и осознанно применялись на практике (разумеется, довольно узким кругом лиц) методы криптографии, стеганографии и кодирования. Как было показано в предыдущем разделе, стеганография и кодирование использовались и ранее в Древней Греции, а вот осознанное применение шифров для практических нужд демонстрирует определенный сдвиг в осознании функционального назначения известных способов преобразования письменных текстов римлянами по сравнению с греками.

7. Стойкость античных шифров с позиций современной математической теории

В предыдущих разделах ставилась задача рассмотреть функции древней тайнописи и смежных с ней способов преобразования текстов, а также социальные аспекты их использования, избегая неоправданной модернизации их конструкций и условия применения. В настоящем разделе,

напротив, делается попытка проанализировать конструкции, свойства и стойкость этих шифров с позиций современной науки, вне зависимости от того, осознавались ли эти способы в древности как шифры или нет (при анализе используются материалы работы [13, с. 3–20]).

Итак, все рассмотренные выше способы и средства преобразования текстов можно классифицировать либо как шифры простой замены (как было показано, их следует считать самыми древними), либо как шифры перестановки, что вытекает из требований взаимной однозначности и обратимости преобразований зашифрования и расшифрования симметричной криптосистемы. Однако все без исключения античные шифры являются лишь частными случаями одного из этих двух классов шифров.

Пусть P — пространство открытых текстов, C — пространство шифртекстов, K — пространство ключей, Z_m — кольцо вычетов по модулю m, k — ключ зашифрования/расшифрования, $e_k(x)$, $d_k(y)$ — уравнения зашифрования и расшифрования соответственно.

Начнем с анализа *шифра сдвига*. Пусть для определенности в шифре используется латинский алфавит, состоящий из 26 букв. Тогда $P = C = K = Z_{26}$. Для $0 \le k \le 25$ уравнения шифрования определяются как $e_k(x) = (x + k) \bmod 26$, $d_k(y) = (y - k) \bmod 26$, где $x, y \in Z_{26}$. При $k = 3$ получаем легко узнаваемый шифр Цезаря. В основе шифра сдвига лежат операции в аддитивной группе кольца вычетов по модулю m. Ключом шифра является величина сдвига алфавита шифртекста относительно алфавита открытого текста, то есть мощность множества ключей также равна $m - 1$ (исключая нулевой сдвиг, который соответствует тождественному преобразованию). Стойкость такого шифра пропорциональна средней сложности задачи тотального опробования всех ключей, которая будет равна $(m-1)/2$, то есть в данном случае $(26-1)/2 = 12,5$. Очевидно, что ключевое пространство такого шифра очень невелико и, имея догадку об использовании шифра сдвига, вскрыть его довольно легко.

Шифр сдвига — частный случай *шифра замены*. Пусть по-прежнему используется латинский алфавит: $P = C = K = Z_{26}$. Пространство ключей K состоит из всех возможных перестановок 26 символов. Для каждой перестановки $\pi \in K$ имеем: $e_\pi(x) = \pi(x)$, $d_\pi(y) = \pi^{-1}(y)$, где π^{-1} — перестановка, обратная к π. Число таких перестановок в общем случае равно $m!$, то есть в данном случае $26! \approx 4,0 \cdot 10^{26}$. Известна формула Стирлинга для приближенной оценки $m! \approx \sqrt{2\pi m} \cdot \left(\frac{m}{e}\right)^m$. Стойкость шифра перестановки в общем случае очень высока, но такие шифры еще не были известны в Античности.

Другой частный случай шифра замены — *аффинный шифр*. При $P = C = Z_{26}$ пространство ключей определяется как $K = \{(a, b) \in Z_{26} \times Z_{26} : \text{НОД}(a, 26) = 1\}$. Для $k = (a,b) \in K$ уравнения шифрования определяются как $e_k(x) = (ax + b) \bmod 26$, $d_k(y) = a^{-1}(y - b) \bmod 26$, где $x, y \in Z_{26}$. Шифр Цезаря является частным случаем аффинного шифра для $a = 1$, $b = 3$. Количество ключей аффинного шифра над Z_m соответствует количеству пар чисел (a,b), при которых функция $y = ax + b \pmod m$ является биективной, и, таким образом, равно $m\varphi(m)$, где $\varphi(m)$ — функция Эйлера (количество целых чисел, меньших m, взаимно простых с m). Напомним, что для $m = \prod_{i=1}^{n} p_i^{e_i}$, где p_i — попарно взаимно простые числа и $e_i > 0$, $1 \le i \le n$: $\varphi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1}\right)$. Стойкость аффинного шифра достаточно высока (по меркам донаучной криптографии), но все же многократно ниже, чем стойкость шифра замены в общем случае.

Наконец, рассмотрим *шифр перестановки*. Пусть m — положительное целое число, $P = C = (Z_{26})^m$, и пространство ключей K состоит из всевозможных перестановок множества чисел $\{1, 2, \ldots, m\}$. Для каждого фиксированного ключа перестановки π уравнения шифрования определяются как $e_\pi(x_1, \ldots, x_m) = (x_{\pi(1)}, \ldots, x_{\pi(m)})$, $d_\pi(y_1, \ldots, y_m) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(m)})$, где π^{-1} — обратная (инверсная) к π перестановка. Напомним, что ярким примером шифра перестановки является скитала. Для скиталы ключом является диаметр цилиндра, на который наматывается лента, но точная оценка

числа ключей для скиталы невозможна, так как она зависит от множества факторов: диаметра цилиндра, ширины ленты, плотности нанесения текста и т. п. На практике представляют интерес лишь те перестановки, которые не оставляют неизменными буквы алфавита открытого текста, то есть такие ключи, которые являются перестановками без неподвижных точек. В комбинаторике такие перестановки принято называть беспорядками. Количество всех беспорядков порядка m может быть вычислено с помощью принципа включения-исключения и задается выражением $!m = \sum_{k=0}^{m} (-1)^k \frac{m!}{k!}$, которое называется субфакториалом числа m. Количество беспорядков $!m = d(m)$ удовлетворяет рекурсивным соотношениям $d(m) = (m-1)\cdot\left(d(m-1) + d(m-2)\right)$ и $d(m) = md(m-1) + (-1)^m$, где $d(1) = 0$, $d(2) = 1$. Ввиду того, что $\sum_{k=0}^{\infty} (-1)^k \frac{1}{k!} = \frac{1}{e}$, значение $!m$ с ростом m ведет себя как $\frac{m!}{e}$, и при положительных m его можно представить как результат округления числа $\frac{m!}{e}$. В случае $m = 26$ число беспорядков равно $!26 \approx 1{,}5 \cdot 10^{26}$. Таким образом, в общем случае стойкость шифров замены, как и шифров перестановки, весьма высока. Однако ни в одном из античных шифров (и шифровальных устройств) общий случай замен и (или) перестановок не реализовывался, а используемые в них частные случаи, как было показано выше, очень существенно снижают стойкость шифров.

Итак, сделаем выводы: в древности эмпирическим путем были «нащупаны» основные принципы шифрования — замены и перестановки символов текста. Но реализованы они были лишь для тех простых частных случаев, которые с позиций современной теории являются криптографически нестойкими, — «стойкость» таких способов преобразования текстов базировалась на ограниченности круга людей, владевших грамотой, и их психологической неготовности к восприятию текста, лишенного семантики и записанного с нарушением правил естественного языка. Более сложные методы дешифрования, основанные на анализе частоты встречаемости символов в шифртексте, в античные времена еще не были известны.

Заключение

Проведенное исследование позволяет сделать следующие основные выводы.

1. Практически всем древним цивилизациям известна тайнопись как особое языковое явление, фиксирующее на материальных носителях существовавшие с незапамятных времен в различных социальных группах «тайные языки». Эти языки имели ритуально-магическое происхождение, но позднее были осознаны как инструмент социальной коммуникации. В связи с этим в период Древней истории тайнопись имела две основные сферы применения:

- «магическую» — для сокрытия тайного смысла имен, магических обрядов, тайных ритуальных знаний и прочих табуированных сведений, то есть для тайных коммуникаций со сверхъестественными силами (что было неотъемлемой частью жизни всех древних цивилизаций);
- «практическую» — для защиты военных донесений, переписки личного характера, а также, возможно, производственных секретов, то есть для тайных коммуникаций в человеческом обществе.

2. В Древнем мире эмпирическим путем открыты важнейшие принципы шифрования: замена и перестановка символов. В античном мире ими фактически исчерпывался арсенал криптографических приемов защиты письменных текстов, да и реализованы они были лишь для простых частных случаев. Эволюция приемов тайнописи происходила крайне медленно из-за отсутствия объективной необходимости их совершенствования.

3. Наряду с тайнописью, а иногда и совместно с ней античные цивилизации пользуются различными способами физической защиты сообщений, их кодирования и приемами стеганографии, которые служат разным практическим целям: сокрытию самого факта существования или передачи сообщения, сокрытию истинных имен отправителей или получателей сообщений, ускорению записи текста и сокращению объемов материального носителя для его записи, передаче сообщения со скоростью, превышающей возможности передвижения человека, повышению значимости текста для читателя. Эти цели зачастую рассматриваются как более приоритетные по сравнению с сокрытием смысла сообщения от непосвященных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Запечников С. В.* Из истории криптографии: тайнопись как явление древнерусского литературного языка (XII—XVII в.) // Безопасность информационных технологий. 2011. № 2. С. 116—123.
2. *Геродот.* История [Электронный ресурс] / Пер. и примеч. Г. А. Стратановского; Под общ. ред. С. Л. Утченко. URL: http://ancientrome.ru/antlitr/herodot/index.htm (дата обращения: 03.02.2014 г.).
3. *Эней Тактик.* О перенесении осад / Пер., ст. и прим. В. Ф. Беляева // Военное искусство античности. М.: Эксмо, 2003. С. 38—106.
4. *Полибий.* Всеобщая история. В 2 томах. Том 1. Книги 1 — 10 / Пер. с греч. Ф. Мищенко; сост. А. Лактионов. М.: Изд-во «АСТ», 2004. — 768 с.
5. *Плутарх.* Сравнительные жизнеописания [Электронный ресурс]. URL: http://krotov.info/acts/02/plu/tarh_lisandr.htm (дата обращения: 26.01.2014 г.).
6. *Светоний Г. Т.* Жизнь двенадцати цезарей / Пер. с лат., предисл. и послесл. М. Гаспарова. М.: Худож. лит., 1990. — 225 с.
7. *Соболева Т. А.* Тайнопись в истории России (История криптографической службы России XVIII — начала XX в.). М.: Междунар. отношения, 1994. — 384 с.
8. *Кан Д.* Взломщики кодов / Пер. с англ. А. Ключевского. М.: Центрполиграф, 2000. — 473 с.
9. *Mollin R.* Codes: The guide to secrecy from Ancient to Modern Times. New York: Taylor & Francis Group, 2005. — 700 p.
10. *Bauer F.* Decrypted secrets: Methods and maxims of cryptology. 4th ed. Berlin: Springer, 2007. — 524 p.
11. *Русецкая И. А.* История криптографии в Западной Европе в раннее новое время. СПб.: Центр гуманитарных инициатив; Университетская книга-СПб, 2014. — 144 с.
12. *Bauer C.* Secret history: the story of cryptology. London: CRC Press, 2013. — 594 p.
13. *Stinson R. L.* Cryptography Theory and Practice. 3rd ed. London: CRC Press, 2006. — 611 p.
14. *Раушенбах Б. В.* Постскриптум. М.: Аграф, 2011. — 304 с.
15. *Фрэзер Дж.* Золотая ветвь. М.: Политиздат, 1986. — 706 с.
16. The Vatsayayana Kama Sutra: The classic translation of 1883 [электронный ресурс] / translated by R. Burton. URL: http://www.classicly.com/books/the-kama-sutra-of-vatsayayana/download_in_format/pdf (дата обращения: 19.05.2014 г.).
17. *Молчанов А. А.* Таинственные письмена первых европейцев. М.: Наука, 1980. — 119 с.
18. *Откупщиков Ю. В.* Фестский диск: Проблемы дешифровки. СПб.: Изд-во СПбГУ, 2000. — 40 с.
19. *Диринтер Д.* Алфавит / Пер. с англ.; общ. ред., предисл. и примеч. И. М. Дьяконова. Изд. 2-е. М.: Едиториал УРСС, 2004. — 656 с.

REFERENCES:

1. *Zapechnikov S. V.* Cryptography as the phenomenon of Russian literature language (XII — XVII centuries) / S.V. Zapechnikov // Security of Information Technologies. 2011. № 2. P. 116—123. (in Russian)
2. *Herodotus.* History. In 2 Vols. Vol. 1. Books 1 — 10 (Russian translation by F. Mishchenko, ed. A. Laktionov). M.: AST, 2004. — 768 pp.
3. *Aeneas Tacticus.* How to Survive Under Siege (Russian translation by V. Belyaev) // Voennoye iskusstvo antichnosti. M.: Eksmo, 2003. P. 38—106.
4. *Polybius.* The General History in 40 books. Book the 2nd (Russian translation form original Greek by F. Mishchenko). SPb, 1995.
5. *Plutarch.* Lives (Russian translation from original Greek). URL: http://krotov.info/acts/02/plu/tarh_lisandr.htm (date of reference: 26.01.2014 г.).
6. *Suetonius H. T.* Lives of the Caesars (Russian translation by M. Gasparov). M.: Hudozhestvennaya literatura, 1990. — 225 p.
7. *Soboleva T. A.* Taynopis' v istorii Rossii (Istoriya kriptograficheskoy sluzhby Rossii XVIII — nachala XX v.). M.: Mezhdunarodnye otnosheniya. 1994. — 384 p.
8. *Kahn D.* The codebreakers (Russian translation by A. Klyuchevsky). M.: Tsentrpoligraf, 2000. — 473 p.
9. *Mollin R.* Codes: The guide to secrecy from Ancient to Modern Times. New York: Taylor & Francis Group, 2005. — 700 p.
10. *Bauer F.* Decrypted secrets: Methods and maxims of cryptology. 4th ed. Berlin: Springer, 2007. — 524 p.
11. *Rusetskaya I. A.* Istoriya kriptografii v Zapadnoy Evrope v rannee novoe vremya. SPb.: Tsentr gumanitarnyh initsiativ; Universitetskaya kniga-SPb, 2014. — 144 p. (in Russian)
12. *Bauer C.* Secret history: the story of cryptology. London: CRC Press, 2013. — 594 p.
13. *Stinson R. L.* Cryptography Theory and Practice. 3rd ed. London: CRC Press, 2006. — 611 p.
14. *Raushenbach B. V.* Postscriptum. M.: Agraf, 2011. — 304 p. (in Russian)
15. *Frazer J. G.* The golden Bough (Russian translation). M.: Politizdat, 1986. — 706 p.
16. The Vatsayayana Kama Sutra: The classic translation of 1883 / translated by R. Burton. URL: http://www.classicly.com/books/the-kama-sutra-of-vatsayayana/download_in_format/pdf (дата обращения: 19.05.2014 г.).
17. *Molchanov A.* Tainstvennye pismena pervyh evropeytsev. M.: Nauka, 1980. — 119 p. (in Russian)
18. *Otkupshchikov Y.* Festskiy disk: Problemy deshifrovki. SPb.: Sankt-Peterburgsky Universitet, 2000. — 40 p. (in Russian)
19. *Diringer D.* A history of the alphabet. 2nd ed. (Russian translation by I. Dyakonov). M.: Editorial URSS, 2004. — 656 p.