С. В. Запечников

ИЗ ИСТОРИИ КРИПТОГРАФИИ: ЗАЩИТА ДОКУМЕНТОВ, ТАЙНОПИСЬ И ТАЙНЫЕ КОММУНИКАЦИИ В ВИЗАНТИИ (IV–XV в.)

Введение

Византия — великая держава, просуществовавшая одиннадцать веков (330–1453 г.). Ей принадлежит выдающееся место в политической, экономической, военной истории, в истории культуры, науки и религии. Одна из областей жизни Византийской империи, которая до настоящего времени остается почти не исследованной, — это история развития в ней тех знаний, которые в наше время составляют предмет науки криптографии, т. е. сфера защиты документов, тайнописи и тайных коммуникаций. В особенности сказанное относится к предыстории криптографического протокола, которая, как представляется, с точки зрения современной науки до сих пор не изучалась. Это тем более парадоксально, что слово «криптография» — греческого происхождения (от др.-греч. κρυπτ$\bar{o}$ς — тайный, скрытый + γρ$\bar{a}$φω — пишу). Сам по себе факт существования такого термина в греческом — родном языке ромеев (это самоназвание византийцев) — уже говорит о том, что обозначаемое им явление занимало определенное место в общественной и культурной жизни империи.

Причин слабой изученности истории криптографии в византийский период мы касаемся в этой статье далее. Также будет показано, что практическая деятельность византийцев в этой области концентрировалась в первую очередь в сферах административного управления империей, внешней политики, дипломатии и военного дела — этим объясняется выбор источников, использованных для исследования.

Настоящей статьей автор продолжает серию публикаций о наиболее заметных этапах исторического развития криптографии, начатую работой [1], ставя своей целью «докопаться до корней» и попытаться отследить истоки формирования современных концепций защиты информации, которые, на первый взгляд, теряются где-то в глубине веков. Еще одна цель заключается в том, чтобы «навести мосты» между средневековыми знаниями, которые еще зачастую не разделялись на науку, ремесло, магию, религию и др., и современными строго научными подходами к решению технических задач, не отделимыми от формально-логических и математических методов исследования; проследить, говоря о сфере защиты информации и криптографии, непрерывную цепь эволюции, связывающую древность и современность.

Вместе с тем автор видит задачу этой работы не в том, чтобы дать абсолютно корректные, с точки зрения историков, ответы на затрагиваемые здесь вопросы развития культуры в Византии, но только лишь в том, чтобы поставить задачу соответствующего исследования и попытаться обозначить некоторые направления поиска ответов на возникающие в рамках этой проблемы вопросы. Особенность предлагаемой работы в том, что здесь предпринимается попытка отследить скорее историю идей в области криптографии и других способов защиты документов, чем историю фактов. Тщательный сбор и анализ фактов, выдвижение на их основе вполне обоснованных гипотез и построение достоверных выводов — это предмет будущих исследований.

Автор надеется, что настоящая статья будет способствовать пробуждению интереса криптографов, математиков, специалистов по информационной безопасности к истории своей науки.

1. Источники по истории криптографии в Византии

Подлинных византийских документов до настоящего времени во всем мире сохранилось сравнительно немного, но достаточно для того, чтобы они могли служить материалами исследований. В большинстве своем они дошли до нас не благодаря, а вопреки всем перипетиям истории, а потому

носят несистематический, скорее случайный характер, тем не менее представляя величайшую историческую ценность. Достаточно напомнить, что Византия, и в особенности ее столица Константинополь, дважды переживали катастрофический разгром с тотальным уничтожением всех институтов государственной власти (не говоря уже о более «мелких» исторических коллизиях): в 1204 г., при завоевании войсками Четвертого крестового похода, и в 1453 г., при штурме города турецкими войсками, что положило конец существованию Византии как государства.

Исключением из этого правила являются лишь сохранившиеся с минимальными потерями с византийского времени до наших дней архивы монастырей горы Афон, а также монастыря Иоанна Богослова на о. Патмос и монастыря св. Екатерины на Синае. Самоуправляемый регион на полуострове Афон в составе современной Греции, нередко также называемый «монашеской республикой Святой горы Афон», является своеобразным культурным реликтом давно уже не существующей Византии в современном мире. Остальная часть уцелевших документов, принадлежащих византийской истории, хранится в архивах Ватикана, Рима, Неаполя, Венеции, Парижа, Милана, Модены, Дубровника, ряда американских и западноевропейских университетов, а потому труднодоступна для российских исследователей.

Работа с первоисточниками, разумеется, была бы наиболее информативна для изучения атрибутов документов, порядка их оформления, способов защиты от подделки и т. п., в том числе и для ответа на один из основных интересующих нас вопросов, который пока остается открытым: в каком объеме сохранились до наших дней документы с образцами византийской тайнописи (в оригинале или в копиях). Во всяком случае, ни в одном историческом исследовании, с которыми ознакомился автор настоящей статьи, не встретилось каких-либо упоминаний о существовании в наше время и местонахождении таких документов. Возможно, что ссылки на них удастся обнаружить при более тщательном изучении вопроса.

В этих условиях роль наиболее информативных источников, из которых мы можем черпать сведения о криптографии в Византии, берут на себя дошедшие до наших дней, опубликованные и хорошо известные историкам сочинения византийских писателей, государственных деятелей, дипломатов, иерархов православной церкви, а также византийские хроники и своды законодательных актов. Косвенные данные можно также получить из хроник и архивных документов сопредельных с Византией стран Восточной и Западной Европы. Большой массив такого рода источников и крайне редко встречающиеся в них сведения об интересующем нас предмете создают немалые трудности при попытках исследования византийской криптографии. К счастью, задача облегчается тем, что за последние годы изданы сборники документов по истории Византии, в том числе в электронном виде, такие как хрестоматия [2], в которой, в отличие от ранее предпринятых изданий, приведены не отрывки, а полные тексты сочинений и документов общим объемом около 28 тысяч страниц.

Из представленного в хрестоматиях классического наследия наибольшую ценность для исследования имеют сочинения византийских государственных деятелей и дипломатов. Так, сведения о дипломатии ранней Византии (IV — первая половина VII в.) мы получаем из произведений Приска Панийского (V в.), Петра Патрикия (VI в.), Нонноса (VI в.), Феофана Византийца (VI в.), Менандра Протиктора (конец VI — начало VII в.), о военно-теоретической мысли — из двух главных трактатов этого периода: «Византийского Анонима VI в.» и «Стратегикона Маврикия». Самые ценные для нас источники по средневизантийскому периоду (вторая половина VII — XII в.) — это трактаты императора Константина VII Багрянородного (913–959), свидетельства епископа Лиутпранда Кремонского (920–972), французского хрониста XII в. Одо Дейльского. Наконец, о поздней Византии (XIII — первая половина XV в.) мы узнаем из «Истории» Никиты Хониата — крупнейшего византийского писателя, историка и политического деятеля конца XII — начала XIII в. и из сочинений его продолжателя Георгия Акрополита (1217–1282).

Значительный интерес представляют ставшие классическими труды российских византинистов Ф. И. Успенского, А. А. Васильева, А. П. Каждана, И. П. Медведева, З. В. Удальцовой, Г. Г. Литаврина.

Среди работ, опубликованных сравнительно недавно, исключительное значение имеют изданные Академией наук СССР коллективные труды [3] и [4–6]. По прошествии многих лет их по праву можно отнести к высшим достижениям советской гуманитарной науки.

Не заменимыми для исследования являются материалы, опубликованные в сети Интернет. Большую подборку ссылок на публикации по истории и культуре Византии, словари, дискуссионные площадки, исследовательские группы и университеты содержит ресурс [7], среди них ссылки на несколько проектов по оцифровке сохранившихся византийских свитков и рукописных кодексов, позволяющих широкому кругу исследователей получить доступ к содержанию бесценных, но недоступных для них первоисточников.

Анализ состава и состояния источников свидетельствует, что практически все выводы по исследуемому предмету могут носить характер более или менее правдоподобных, но все-таки дискуссионных гипотез и пока вряд ли могут рассматриваться как твердо установленные научные факты. Возможно, этим объясняется то, что исследователи, проявляющие интерес к истории криптографии, до сих пор обходили молчанием историю криптографии в Византии.

2. Функции криптографии в Византии

Византия имела очень развитую и многофункциональную административную систему, которую обслуживал огромный чиновничий аппарат. Это обусловливало появление громадного количества документов, сопровождавших функционирование аппарата государственного управления, церковных властей, военной машины, дипломатии и других ведомств. Номенклатура известных византийских документов весьма велика: от императорских указов и сводов законодательных актов до монастырских уставов и документов о праве собственности на недвижимое имущество. Система обращения документов в империи была выстроена на достаточно высоком уровне: так, достоверно известно о существовании в Византии института нотариата и целой системы государственных, церковных и частных архивов, о государственной регистрации прав и наиболее важных документов. Учитывая столь большое значение документа, надо полагать, что и проблема защиты документов в Византии была весьма актуальна.

Условимся в рамках данной статьи различать употребление слов «тайнопись» и «защита документов». Под тайнописью будем понимать собственно способы преобразования текстов с целью сделать их нечитаемыми, непонятными для непосвященных, т. е. те или иные формы шифров. Под защитой документов станем понимать в широком смысле всю совокупность способов защиты документов от нежелательного прочтения, подделки, подлога, несвоевременного уничтожения. Все эти задачи в настоящее время относят к сфере криптографической защиты информации, поэтому представляется правомерным, исследуя историю криптографии, рассматривать не только историю тайнописи, но и историю развития всех известных способов защиты документов.

Такая постановка задачи тем более справедлива, что, как мы увидим далее, в Византии уже в той или иной форме осознанно или неосознанно использовались все те же самые функции защиты информации, которые известны современной науке, — это обеспечение секретности, подлинности, целостности и доступности документов. Секретность документов обеспечивалась применением тайнописи и существованием системы тайных коммуникаций, целостность и подлинность — подписями и печатями на документах, а доступность (в рассматриваемом контексте скорее интерпретируемая как сохранность) — копированием и архивацией наиболее значимых документов.

Дальнейшая структура статьи сформирована таким образом, чтобы подробнее рассмотреть все основные аспекты защиты документов в Византии, проследить историю формирования

концепций защиты информации и зафиксировать связи с современностью: пп. 3—4 посвящены тайнописи, п. 5 — системе тайных коммуникаций, п. 6 — подписи и печати на документах, п. 7 — архивам Византии, п. 8 — такому интересному феномену, как византийский дипломатический протокол, наконец, в п. 9 рассматриваются современные интерпретации задач защиты информации, использующие выработанные в Византии идеи.

3. Сферы применения тайнописи

Анализ источников позволяет установить два принципиально различных и даже противостоящих друг другу направления применения тайнописи в Византии. Во-первых, это применения в интересах органов государственной власти и административного управления империей — условно говоря, «государственные» применения. Во-вторых, это разного рода применения тайнописи в целях сокрытия той или иной информации от официальных лиц государства и церкви — то, что условно можно было бы назвать «антигосударственными» применениями.

Первое направление — «государственные» применения — в свою очередь, включает в себя две сферы: дипломатию и военное дело. Ни для кого не секрет, что тайнопись и шифры всегда играли важную роль в дипломатии, этот тезис остается справедливым и в наши дни. А Византия, как известно, создала самую влиятельную, высокоорганизованную и изощренную дипломатическую систему в Европе и на Ближнем Востоке, которая оставалась таковой вплоть до XIII в. [5. Гл. 8]. По мнению многих византинистов, именно благодаря своей дипломатии Византия была столь жизнеспособным политическим образованием, что смогла просуществовать более тысячи лет, при этом всегда оставаясь центром сложных международных коллизий [4. Гл. 9]. Не война, а дипломатия всегда была для империи главным инструментом ее отношений с другими странами и народами.

Чтобы выделить функции, которые выполняла тайнопись для византийской дипломатии, нужно обратить внимание на следующие факты.

Во-первых, вплоть до конца XIII — начала XIV в., т. е. практически до сбмого конца существования Византии как государства, в международной практике не было принято назначать постоянных послов одного государства в другом государстве (впервые в мире постоянными послами стали нунции Папы Римского в католических странах Западной Европы). Послы направлялись императором Византии в другую страну временно для решения конкретной задачи международной политики, при этом сроки пребывания посла в другой стране с учетом длительных переговоров, долгих переездов и условностей дипломатического протокола могли быть весьма значительными — несколько месяцев, иногда даже несколько лет. В этих условиях большое значение имели письменные коммуникации как единственная возможность для поддержания связи с родиной, а также для докладов послов и получения ими указаний императора и чиновников. Разумеется, такого рода переписка не предназначалась для посторонних глаз, поэтому применение тайнописи здесь было просто необходимо.

Во-вторых, именно византийская дипломатия впервые стала совмещать свои функции с функциями внешней разведки. «Помимо письменной инструкции, послы получали также устную, которая давалась обычно в секретном порядке. Иногда посольству, помимо официальных поручений, давалось задание разузнать о политической ситуации и настроениях при иностранном дворе. Так дипломатия сочеталась с политической и военной разведкой» [5. С. 255]. Разумеется, для выполнения этих специфических задач тем более необходим такой инструмент обеспечения безопасности, как тайнопись.

В-третьих, известной особенностью Византии наряду с блестящей «официальной» дипломатией была ее тайная дипломатия, которая использовала данные, собранные внешней разведкой. «В сложной международной обстановке того времени Византия не брезговала для достижения своих целей любыми средствами. Мемуары византийских дипломатов, даже самых честных и правдивых,

показывают, как по требованию правительства им приходилось прибегать к подкупу иноземных правителей, плести заговоры при иноземных дворах, натравливать одни народы на другие. Византийская дипломатия руководствовалась своего рода кодексом вероломства: ее девизом по-прежнему оставался испытанный принцип политики римлян: "Разделяй и властвуй!"» [4. С. 379]. Одним из характерных эпизодов, где проявилось действие византийской тайной дипломатии, были ее отношения с Русью в X в.: открытая сторона дипломатии при этом состояла в том, что между Византией и Русью шли переговоры и было заключено три официальных договора 907, 944 и 971 г. «Втайне же, следуя вероломному кодексу византийской дипломатии, Византия натравила на Святослава печенегов и подготовила тем самым его гибель в днепровских порогах весной 972 г.» [5. С. 268]. В поздней Византии с ослаблением империи эта сторона дипломатической деятельности только усилилась. «Традиционными восходящими к предшествующим столетиям были и такие средства дипломатии XIII–XIV в., как... сознательный выбор для следования послов через страну кружного труднопроходимого пути... засылка шпионов во враждебную страну, тайные посольства и секретные договоры. Тайная дипломатия расцвела особенно в XIV в.» [6. С. 348]. Византийская дипломатия знала и успехи, и промахи. Однако очевидно, что подобная деятельность всегда была сопряжена с большим риском: в частности, был крайне нежелателен и опасен перехват дипломатической информации представителями тех стран и народов, против которых были направлены «козни» тайной дипломатии.

Таким образом, византийская дипломатия имела более чем достаточно причин для использования тайнописи в своей деятельности.

В военном деле функции тайнописи, по-видимому, были традиционны и состояли в обеспечении секретности передачи приказов и иных письменных сообщений между военачальниками, действующими совместно в составе одной армии, а также между военачальниками и императором (императорской канцелярией).

Существование второго направления применения тайнописи, которое мы назвали «антигосударственным», устанавливается по обрывочным сведениям и даже намекам, содержащимся в произведениях византийских писателей, и ссылкам на них исследователей истории Византии. Сюда мы относим тайнопись, применявшуюся при переписке книг, содержание которых противоречило официальным доктринам государства и (или) вероучению православной церкви: сочинений по астрологии, магии, еретических трактатов. Очевидно, что обнаружение подобных книг или записей в открытом виде могло повлечь самые нежелательные последствия для их владельцев. Достоверных исторических сведений об этой «темной» стороне византийской жизни, по-видимому, уже не сохранилось. Однако, по некоторым данным, с целью искоренения ересей и сама тайнопись также причислялась властями Византии к чернокнижию и колдовству. Разумеется, учитывая двойные стандарты византийской государственной машины, такая квалификация тайнописи не могла относиться к дипломатическим и военным шифрам, а касалась лишь гражданской сферы, точнее говоря, лишь рядовых граждан.

Таким образом, коренное различие двух направлений, о которых шла речь выше, состоит в следующем: в «государственных» применениях тайнопись была встроена, «обернута» в соответствующую инфраструктуру — систему тайных коммуникаций, являясь органической частью дипломатического и военного искусства; этого, разумеется, не наблюдалось в «антигосударственных» применениях.

4. Способы тайнописи

Сведения о способах тайнописи в Византии весьма разрозненны и отрывочны. Они восстанавливаются почти исключительно по косвенным источникам, главными из которых являются образцы тайнописи из стран, входивших в орбиту влияния Византии (или, как стало

принято говорить среди историков, в «Византийское содружество»). В основном это южно-, западнославянские и древнерусские памятники письменности. Учитывая традиционно большое влияние Византии на все сферы общественной и культурной жизни стран восточноевропейского ареала, есть основания полагать, что подавляющее большинство способов и форм тайнописи было заимствовано представителями славянских народов из византийских первоисточников.

В среде славянских народов начиная с XII—XIII в. было достаточно грамотных людей, знавших в том числе и греческий язык, что позволяло им, усвоив способы тайнописи в первоисточнике, перенести их на свои родные языки. Принимая предположение о том, что сами способы древнерусской и южнославянской тайнописи в основном были заимствованы из греческого языка (транслировались, разумеется, только способы, которые как бы «переводились» на славянские языки), наиболее полную систематизацию способов византийской тайнописи можно построить на основе систематизации способов славянской тайнописи, предложенной выдающимся русским филологом М. Н. Сперанским в [8]. Единственное изменение будет состоять в исключении тех видов тайнописи, которые сам М. Н. Сперанский называет заведомо невозможными для греческого языка.

Таким образом, получается следующая систематизация способов византийской тайнописи.

1. Замена греческого алфавита иными алфавитами: латинским, арабским, кириллицей, глаголицей — это наиболее «слабый» из всех способов тайнописи.

2. Система измененных начертаний символов, деформация обычных букв, сильно измененная скоропись, делающая записи похожими на иноязычные тексты.

3. Система замен и перестановок символов греческого алфавита: простая замена, полиалфавитная подстановка и др.

4. «Цифровая тайнопись» — замена обычных букв иными на основе их численного значения. В греческом языке до усвоения ромеями арабской системы нумерации большинству букв соответствовали и цифровые значения, так что они применялись для нумерации и счета. Этот же способ был заимствован славянскими языками: буква со знаком титла над ней принимала значение числа. Таких способов византийцам могло быть известно по меньшей мере четыре:

а) «разложение суммы»: числовое значение затаиваемой буквы разлагается на два или несколько слагаемых — соответственно этому заменяются буквы;

б) описательная система: словами излагается порядок букв-цифр, составляющих слово, и указываются арифметические действия, которые с ними следует выполнить, чтобы прочитать исходные слова;

в) «точечная тайнопись»: к обычной букве открытого текста прибавляют или от нее отнимают несколько единиц, десятков или сотен ее цифровой значимости и пишут результат этого буквой шифртекста, обозначая точками, сколько надо отнять или прибавить к ее цифровому значению, чтобы получить исходную букву открытого текста;

г) «афонская» тайнопись (по месту изобретения в монастырях на Афоне): взаимная замена букв, дополняющих одна другую по своему числовому значению до 10, 100 или 1000.

5. Акростих — особая форма стихотворных текстов, где исходный открытый текст читался по буквам, стоящим на определенных позициях (чаще всего — в начале каждой строки).

6. Обратное и фигурное письмо — всевозможные нарушения обычного порядка следования букв в тексте, затруднявшие для непосвященных понимание смысла.

7. «Лигатурное письмо» (вязь, монокондил) — особые фигурные знаки, позволяющие опознать писца или адресата, как правило, ставившиеся в начале или в конце документа, прообраз современной собственноручной подписи.

8. Комбинированные способы тайнописи.

За детальным описанием всех перечисленных способов отсылаем читателя к [8].

Здесь уместно повторить один из выводов, сделанных автором настоящей работы в статье [1]. Принципиально важный момент, на наш взгляд, заключается в том, что средневековая тайнопись — это явление, относящееся к сфере языкового сознания носителей языка, но отнюдь не к сфере техники или математики (пусть даже понимаемых в самых элементарных формах). Этот вывод ранее был сделан на материале древнерусской тайнописи, но с уверенностью можно полагать, что он справедлив и для византийской тайнописи, и тому есть несколько причин. Во-первых, византийская культура (и византийская литература в особенности!) в течение многих веков была образцом, авторитетом и потому источником заимствований для Древней Руси. Во-вторых, в этом убеждают сведения об уровне развития математических знаний в Византии. Несмотря на то что о византийской математике известно очень мало (даже в таком авторитетном издании, как [9], математике в Византии посвящено менее двух страниц), историки единодушно сходятся во мнении о том, что при достаточно заметном вкладе Византии в другие науки математика там получила весьма слабое развитие. Империя скорее выступала в качестве транслятора математических знаний Античности и арабского Востока для Западной Европы, но собственных достижений в этой сфере почти не имела. Наконец, в-третьих, анализ всех известных средневековых шифров, не только древнерусских, но и западноевропейских, показывает, что принцип их действия легко может быть описан вербально или в крайнем случае в таблично-схематической форме, при этом математическое описание по большому счету излишне. Самая сложная «математическая» операция, которая встречается в средневековых (и даже еще раньше — в древнеримских) шифрах, — это циклический сдвиг алфавита влево (вправо) на несколько позиций.

Все это дает основания утверждать, что Византией за всю историю ее существования не было внесено чего-либо принципиально нового в технику шифрования.

5. Система тайных коммуникаций в Византии

Византия имела хорошо организованную систему передачи тайных сообщений, основными пользователями которой были дипломатическое и военное ведомства империи. Материальную основу этой системы образовывала сеть дорог, значительная часть которой была построена еще во времена Римской империи, а также система почтовых станций. Функционирование системы обеспечивала имперская почта. Сеть почтовой связи охватывала практически всю территорию Византии. «Имперская почта, являвшаяся монополией государства, во многом была поставлена на службу внешней политике и дипломатии. Ею ведали сначала магистр оффиций, потом логофет дрома. Он заботился об условиях безопасности и скорости передвижения византийских и иноземных послов и других дипломатов. Дипломаты и чиновники могли в первую очередь пользоваться лошадьми и повозками на почтовых станциях, находить там приют и обеспечение провиантом. Содержание имперских дорог было возложено на население той территории, через которую они проходили» [5. С. 256–257].

Почта обеспечивала самый быстрый способ доставки сообщений и передвижения людей. В связи с этим, по всей видимости, направление специальных посланников или курьеров было необходимо лишь при пересылке сообщений за границу, а также на плохо контролируемые или не контролируемые в текущий момент территории Византии. Логично предположить, что необходимость в таких посланниках возникала лишь на том участке маршрута пересылки сообщений, который не обслуживался государственной почтой.

Из истории известны факты использования методов стеганографии при пересылке сообщений по опасным маршрутам. Напомним, что слово «стеганография» также греческого происхождения (от др.-греч. στεγανός — крыша + γράφω — пишу, т. е. буквально «письмо под крышей») — и обозначает науку о методах сокрытия самогу факта существования какого-либо сообщения. Стеганография всегда существовала как бы «в параллельной плоскости» по отношению к криптографии, и использование тех и других методов никогда не противоречило друг другу.

Стеганография накопила солидный арсенал средств сокрытия сообщений, потому ее история может служить предметом отдельного исследования. В связи с этим подробно останавливаться на методах стеганографии в данной статье мы не будем.

В качестве примера приведем лишь один способ, который широко применялся дипломатическими посланниками разных стран, в том числе Древней Руси. «Русские послы или гонцы везли к иностранному монарху единственную грамоту царя. Если их было две, то одна — фальшивая. Последняя могла быть написана в расчете на запорожцев, если посольство направлялось в Крым или в Стамбул, или на поляков, если оно следовало в Вену или Прагу. При нападении тех или других им следовало отдать подложную грамоту, а вторую — спрятать или уничтожить» [10. С. 267].

6. Роль подписи и печати на византийских документах. Защита документов от подделки

Если тайнопись и тайные коммуникации имели сравнительно узкую сферу применения, то подтверждение подлинности было необходимо для абсолютного большинства документов. Византия во многом являлась родоначальницей тех принципов обеспечения подлинности документов, которые используются по настоящее время для бумажных документов и в трансформированном виде теперь перенесены на электронные документы. Главными средствами подтверждения подлинности были подпись лица, составившего документ, и печать того органа государственной власти или должностного лица, который отвечал за его содержание.

Самыми важными в иерархии византийских документов были, разумеется, грамоты императора (особенно принимая во внимание считавшийся сакральным характер императорской власти). Императорские жалованные грамоты в соответствии с типом формуляра подразделялись на хрисовулы (греч. Χρυσόβουλλον — золотая булла) и простагмы [3. Т. III. С. 6]. Наиболее значительные указы оформлялись как хрисовулы: в них император собственноручно пурпурными чернилами вписывал несколько слов, ставил подпись и дату, после чего хрисовулы скреплялись печатью (иногда отлитой из золота) на шелковом шнурке. (Именно отсюда пошла традиция, которая дожила до нашего времени, в важных письмах, даже подготовленных в машинописном виде, тем не менее, от руки вписывать несколько слов в знак уважения к адресату: как правило, обращение в начале документа и (или) слова «С уважением», «С наилучшими пожеланиями» и т. п. перед собственноручной подписью.) Менее значительные документы оформлялись как простагмы — это вид императорского указа, содержащий прямой приказ к непосредственному исполнению. На них ставилась восковая печать. Простагмы писались обычным шрифтом на бумаге квадратного формата небольшого размера, завершались датой и подписью императора с сокращенным титулом.

Императорской печатью скреплялись и дипломатические договоры Византии, однако процедура заключения и оформления международных договоров была достаточно сложной, о чем подробнее речь пойдет в п. 8. Первоначально подлинность договоров обеспечивалась свинцовыми печатями дипломатов, которые принимали на себя обязательство ратифицировать договор у императора. После утверждения договора императором к нему добавлялась императорская печать. В силу особенностей византийского мировоззрения в период расцвета Византийской империи даже международные договоры во всех возможных случаях старались оформлять как хрисовулы византийского императора.

Распорядительные документы императорской канцелярии назывались «простаксисы». По статусу эти документы были чем-то вроде нынешних постановлений правительства. Были и другие виды документов: экскуссии, рескрипты и пр. Своя система делопроизводства, в том числе подтверждения подлинности документов, существовала и в патриаршей канцелярии, и в административных учреждениях на местах. Впрочем, номенклатура византийских документов, обычаи и правила ведения документооборота заслуживают отдельного рассмотрения.

Весьма интересен тот факт, что византийский опыт атрибутирования документов подписью и печатью впоследствии был воспринят в странах Западной Европы и в государствах восточноевропейского ареала, входивших в орбиту влияния Византии, в частности на Руси. Однако интерпретирован он был по-разному.

Так, в Русском государстве принцип разделения смысловой функции подписи и печати был доведен до своего логического завершения: об ответственности за форму документа свидетельствовала подпись, за содержание — печать. «По представлениям русских людей XV — XVII вв. документ способна атрибутировать только печать. Если соглашение заключалось за рубежом или на посольских съездах, свои печати к "договорной грамоте" прикладывали или привешивали все члены данного посольства, облеченные соответствующими полномочиями, но поставить подпись должен был только дьяк, то есть человек, отвечающий не за сам договор, а за его словесную форму. Подпись закрепляла ответственность лица, "давшего руку" за "букву" документа. Не случайно само выражение "руку дать" означало не только поставить подпись, но и написать весь текст. Об ответственности за содержание документа свидетельствовала печать» [10. С. 274]. Эта традиция прочно закрепилась на Руси и дошла до нашего времени: «бумага без печати — не документ».

Иной порядок атрибутирования документов сложился в западноевропейских странах. «В Западной Европе собственноручная подпись уже в то время имела несравненно большее и иное значение. Вероятно, это было связано с ренессансными представлениями о личности, которая в единстве своего физического и духовного начала является не только объектом Божественного промысла, но и его орудием. Подпись несет на себе следы телесной природы человека, лично утверждающего свою собственную волю, а печать есть лишь символ его социальной роли. Одно дополняет, но не заменяет другое. В 1506 г. послы Максимилиана I привезли в Москву его грамоту, на которой подпись императора стояла в двух местах. Послы объяснили это тем, что вскрылись случаи подделки императорской печати. Следовательно, подпись подтверждала ее подлинность, а не наоборот. Королева Елизавета I в 1583 г. писала Ивану Грозному: "И мы того в сердце свое мысли и в послушанье сего дела приложили есми свою руку". Иными словами, подпись королевы под грамотой подтверждала истинность ее содержания в настоящем и гарантировала исполнение обещанного в будущем, в полной мере представляя собой то, чем она является теперь» [10. С. 275].

7. Архивы Византии. Обеспечение сохранности документов и защита от подлога

Практически единственной отечественной работой, посвященной целенаправленному изучению византийских архивов, является диссертация [11]. В этой работе на основе исследования структуры государственного аппарата Византийской империи сделаны выводы о характере и примерном составе документов, отлагавшихся при византийских учреждениях, а также об основных принципах хранения, использования документов, работы с ними, т. е. по существу — об организации документооборота. Из всего круга вопросов, затронутых в [11] и тех ранее опубликованных работах, на которые ссылается автор, нас интересует, прежде всего, проблема функционирования архивов как одного из институтов защиты документов.

На основе изучения доступных материалов можно сделать выводы о трех основных функциях византийских архивов, имеющих значение для защиты документов.

1. Основной функцией архивов Византии, как и любых других архивов, являлось долгосрочное хранение документов, представляющих ценность для государства и общества, и выдача их по требованиям лиц, имеющих допуск к работе с архивами. В этом смысле функции архивов в аспекте защиты документальной информации заключаются, выражаясь современным языком, в обеспечении сохранности, доступности носителей документов и защите их от несанкционированного доступа.

2. В византийской системе документооборота государственных учреждений важная роль отводилась копированию документов и последующей архивации копий, что было обусловлено как

особенностями византийского делопроизводства, так и стремлением частных лиц, монастырей, других учреждений бережно сохранять акты, имевшие для них жизненно важную ценность. По приводимым в [11] данным, примерно половина византийских актов сохранилась до наших дней именно в виде копий в составе копийных сборников или отдельных свитков. Очевидно, что с точки зрения задач защиты информации копирование документов повышает сохранность их содержания в условиях утраты носителей и обеспечивает более высокую доступность отраженной в документе информации.

3. Далее, как отмечается в [11. С. 15], «в связи с высокой ролью документа в социально-экономической и политической жизни Византии весьма широка была практика подлогов в различных документах, особенно относящихся к имущественным правам. Вместе с тем число подложных документов, откладывавшихся в византийских архивах, все же — если судить по сохранившимся документальным комплексам — можно назвать относительно небольшим. Это было связано со сложностью создания подложного документа, способного пройти проверку на всех административных уровнях (поскольку вся собственность обязательно регистрировалась соответствующими ведомствами: к примеру, все частные пожалования... приобретали силу лишь после регистрации в соответствующем столичном ведомстве и затем — в административном центре той области, где находились пожалованные земли). Такая система была действенной, пока нормально функционировала сама имперская администрация — то есть до начала XIV в.». Таким образом, архивы Византии в совокупности с развитой системой государственных учреждений обеспечивали надежную защиту от подлога документов: даже при наличии подложного документа можно подкупить одного, двух, трех чиновников, но невозможно подкупить всех или это обойдется настолько дорого, что станет невыгодно.

Та же по сути своей система реализуется и в условиях современного компьютеризированного документооборота, когда даже наличие хорошо изготовленного поддельного или исправленного документа не позволяет им воспользоваться, поскольку документ не проходит проверку по всем соответствующим базам данных.

8. Византийский дипломатический протокол как прообраз современного криптографического протокола

Под словом «протокол» (от греч. πρωτόκολλον — первый лист, восходящего к πρωτος — первый, +κολλάω — клею) в ранней Византии понимался листок, приклеенный к свитку папируса, с титульной информацией (дата написания, имя писателя) и кратким содержанием этого свитка. Впоследствии этим термином стали обозначать правила оформления документов и ведения архивов. Позже слово «протокол» стало употребляться применительно к дипломатии и дипломатической службе. Расширилось его содержание: помимо правил оформления дипломатических документов, к дипломатическому протоколу стали относить вопросы этикета и церемониала. По определению современного «Дипломатического словаря», «Протокол дипломатический — совокупность общепринятых правил, традиций и условностей, соблюдаемых правительствами, ведомствами иностранных дел, дипломатическими представительствами, официальными лицами в международном общении» (цит. по [12. С. 23]).

Изучение источников, касающихся истории византийской дипломатии, позволяет с достаточным основанием утверждать, что в «государственных» применениях тайнописи именно дипломатический протокол, а в военной сфере еще и правила и обычаи ведения войны являлись той «оберткой», инфраструктурой применения тайнописи, о которой шла речь выше.

В Византии по существу зародилось и достигло больших высот искусство дипломатического протокола. Не касаясь его церемониальной, этикетной стороны, попытаемся на одном примере проанализировать логику тех действий и процедур, которые выполнялись в соответствии с протоколом. Очень примечателен в этом смысле рассказ Менандра Протиктора о заключении

в 561 г. договора с Ираном. Он перечислил 14 пунктов договора и описал всю процедуру его подписания. «По окончании переговоров, когда стороны достигли договоренности по основным вопросам, был письменно составлен мирный договор сроком на 50 лет. Текст его был написан "по-персидски и по эллински, затем эллинский оригинал был переведен на персидский язык, а персидский — на эллинский"... После написания договора оба текста были сличены друг с другом для установления равноценности содержащихся в них мыслей и формулировок... Когда договор был составлен на двух языках и с него были сняты копии, приступили к последнему этапу. Подлинники мирного договора, представлявшие собой свитки, были скреплены восковыми печатями и другими приспособлениями, которыми обычно пользуются персы, а также отпечатками перстней послов и 12 толмачей — 6 греческих и 6 персидских. Затем произошел обмен текстами договора... На этом церемония подписания договора была закончена... Затем состоялась уплата ромеями персам установленной договором дани» [4. С. 387–388].

Как видим, описанная здесь последовательность действий по существу представляет собой решение хорошо известной современной криптографии задачи. Это «задача одновременного подписания контракта», а в «компьютерной» криптографии она интерпретируется еще и как «задача равноправного обмена цифровыми подписями». Обращает на себя внимание тот факт, что современный «компьютерный» метод решения этой задачи во всех подробностях повторяет византийский способ, только уже на новой технической базе и для новых, цифровых способов представления информации.

Ограниченный объем статьи не позволяет привести другие примеры, но с такой же тщательностью в Византии собиралась разведывательная информация о положении дел в других государствах: использовалось множество независимых источников, каждый перекрестно сопоставлялся с другими, информация перепроверялась, после чего делались окончательные выводы. И этот процесс также был своеобразным византийским дипломатическим протоколом, но уже относился к сфере тайной дипломатии.

9. Византийская криптография и современность

В начале 1980-х годов в связи с бурным развитием компьютерной техники и средств связи в научной литературе по криптографии возникает интерес к задачам обеспечения безопасности при взаимодействии узлов распределенных компьютерных систем. Как ни парадоксально это звучит, но в решении такого рода задач исследователям помогает образное мышление и... знание истории Средневековья. Одна из базовых задач взаимодействия узлов распределенной системы получает название «задача о византийских генералах» [13].

Суть задачи (в неформальной постановке) сводится к следующему: у генерала, командующего армией («генерала армии»), в подчинении находятся $n-1$ генералов («генерал-лейтенантов»), т. е. всего n генералов. Среди генералов могут быть как честные («лояльные»), так и противники («нелояльные»), в том числе и сам командующий. Нужно так построить протокол взаимодействия между ними, чтобы при рассылке генералом армии приказов своим $n-1$ подчиненным генерал-лейтенантам обеспечивалось выполнение следующих условий:

1) все честные генерал-лейтенанты всегда выполняли бы один и тот же приказ;

2) если генерал армии честный, то каждый честный генерал-лейтенант выполнит приказ, который он получает.

В работе [13] показано, что если все сообщения передаются в устной форме, без документа, подтверждающего авторство (т. е. в «компьютерной» трактовке — без цифровой подписи), то «задача о византийских генералах» имеет решение только в том случае, если при заданном числе m «нелояльных» генералов общее количество генералов $n \geq 3m+1$. Если же сообщения передаются в письменной форме, позволяющей обеспечить невозможность отказа от факта

создания и неизменность документа (т. е. в «компьютерной» трактовке — заверены цифровой подписью), то при $n \geq m + 2$.

На базе «задачи о византийских генералах» формулируется «задача византийского соглашения»: для n взаимодействующих генералов нужно предложить такой протокол взаимодействия, чтобы при наличии среди них m «нелояльных» генералов остальные генералы — «лояльные», — имея каждый свое мнение, всегда вырабатывали согласованную общую позицию (например, штурмовать крепость или нет). Принцип решения этой задачи заключается в том, что в протоколе каждый из генералов (в данном случае они равноправны) поочередно выступает в роли командующего, рассылая свое мнение, и в роли подчиненного, собирая мнения других. Процедура голосования по мажоритарному принципу гарантирует, что каждый честный генерал в итоге получит один и тот же результат. Способы решения задачи различаются при пересылке подписанных и неподписанных сообщений.

Мы не знаем достоверно, было ли известно решение этих задач византийцам, но сформулированы они достаточно правдоподобно — интриги, измены, подкуп и предательство, как известно, были повседневным оружием в арсенале средств византийской дипломатии и военного дела. Примечательным здесь представляется тот факт, что спустя несколько веков фактически та же самая задача, которая, вполне вероятно, была актуальна для византийцев, теперь, будучи переформулирована в новом качестве и решена на новой технической базе, послужила основой развития одного из важных направлений современной науки о компьютерной безопасности.

Протокол византийского соглашения является базовым для построения многих других протоколов: достижения консенсуса, частичного соглашения гарантированной широковещательной рассылки и др. Достаточно полный обзор иерархии этих протоколов приводится, например, в [14]. Ежегодно появляется значительное количество новых и усовершенствованных протоколов, решающих все более сложные задачи защиты распределенных систем.

Заключение

Проведенное исследование позволяет сделать следующие основные выводы.

1. Частью высокоразвитой культуры Византийской империи являлась культура документа как особого феномена общественных отношений и связанного с ним документооборота. Документы имели очень важное значение в административной, политической, экономической, финансовой, военной, дипломатической сферах жизни Византии, в связи с чем проблемы защиты документов — сохранения их от преждевременного уничтожения, подтверждения подлинности, предотвращения ознакомления с ними нежелательных лиц — имели первостепенное значение. Византийская культура документооборота послужила источником многих концепций защиты документов, которые остаются актуальными в наши дни и получают новое развитие в электронном документообороте.

2. Обеспечение тайны документов в Византии было актуально в основном в дипломатической и военной сферах, для чего использовался ряд систем тайнописи. Византийская тайнопись, как это типично для Средневековья, принадлежала к сфере языкового сознания носителей языка, но не осознавалась ими как техническое или математическое средство защиты. Тайнопись являлась составной частью византийской системы тайных коммуникаций, применявшейся для решения множества практических задач.

3. Византия была одним из первых в истории государств, где подпись и печать стали использоваться в качестве средств обеспечения достоверности документа, включая целостность его формы и подлинность его содержания. Традиции использования подписи и печати были заимствованы у Византии странами, испытавшими ее влияние. Однако функции и смысл этих средств были интерпретированы по-разному в странах Западной и Восточной Европы, что сохранилось в принятых обычаях оформления документов вплоть до настоящего времени.

4. Долговременная сохранность документов обеспечивалась в Византии развитой системой архивов. Одновременно архивы обеспечивали важную общественную функцию — защиту от подлога документов. Созданные в Византии традиции архивного дела и система многоступенчатой проверки документов административными органами послужила прообразом современной организации документооборота и документационного обеспечения в органах государственной власти.

5. Византийский дипломатический протокол, разработанный за многовековую историю империи с исключительной логичностью, полнотой и тщательностью, во многом стал прототипом современного криптографического протокола (реализуемого, разумеется, для иных целей и на новой технической базе). Рациональное зерно, заимствованное криптографическим протоколом из византийского дипломатического протокола, заключается в логике и механизмах обеспечения максимальной выгоды (максимально благоприятных условий достижения поставленных целей) при полном или частичном недоверии друг к другу участников протокола, которые, тем не менее, заинтересованы в совместном решении некоторой общей задачи.

6. Идеи, запечатленные в византийском письменном наследии и отложившиеся в традициях защиты документов, продолжают служить источником развития современной науки о компьютерной безопасности, в частности, в сфере обеспечения корректного взаимодействия узлов распределенных компьютерных систем. Слабая на сегодняшний день степень изученности византийского документального наследия позволяет предположить, что богатство идей, выработанных Византией в сфере защиты документов, тайнописи и тайных коммуникаций, далеко не исчерпано и в будущем продолжит служить делу развития науки и практики обеспечения информационной безопасности.

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. История Византии. Хрестоматия [эл. ресурс]: Часть I: Историки Византии. Часть II: Исторические документы и исследования. М.: Директмедиа Паблишинг, 2008. 2 CD-ROM. (Историческая библиотека «Клио».)
3. История Византии (в 3-х тт.) / Отв. ред. С. Д. Сказкин. М.: «Наука», 1967. Т. I. — 524 с.; Т. II. — 472 с.; Т. III. — 508 с.
4. Культура Византии. IV — первая половина VII в. / С. С. Аверинцев [и др.]; отв. ред. З. В. Удальцова. М.: «Наука», 1984. — 728 с.
5. Культура Византии. Вторая половина VII — XII в. / С. С. Аверинцев [и др.]; отв. ред. З. В. Удальцова, Г. Г. Литаврин. М.: «Наука», 1989. — 680 с.
6. Культура Византии. XIII — первая половина XV в. / С. С. Аверинцев [и др.]; отв. ред. Г. Г. Литаврин. М.: «Наука», 1991. — 640 с.
7. Культура, наука и искусство // Сайт проекта «Византийская держава»: История и культура государства ромеев. URL: http://www.byzantion.ru/techne/techne.htm (дата обращения: 18.05.2012).
8. *Сперанский М. Н.* Тайнопись в юго-славянских и русских памятниках письма. 2-е изд. М.: Книжный дом «Либроком», 2011. — 168 с.
9. История математики с древнейших времен до начала XIX столетия (в 3-х тт.). Том 1: История математики с древнейших времен до начала Нового времени / И. Г. Башмакова [и др.]; под ред. А. П. Юшкевича. М.: «Наука», 1970. — 352 с.
10. *Юзефович Л.* Путь посла: Русский посольский обычай. Обиход. Этикет. Церемониал. СПб.: Изд-во Ивана Лимбаха, 2007. — 344 с.
11. *Меньшиков А. В.* Архивы Византии X — XV вв. Автореферат дисс. … канд. ист. наук. М.: РГГУ, 2009. — 28 с.
12. *Борунков А. Ф.* Дипломатический протокол в России. 3-е изд. М.: Международные отношения, 2007. — 264 с.
13. *Lamport L., Shostak R., Pease M.* The Byzantine generals problem // ACN Transactions on Programming Languages and Systems. 1982. Vol. 4. P. 382—401.
14. Secure and efficient asynchronous broadcast protocols / C. Cachin [и др.]. URL: http://eprint.iacr.org/2001/006 (дата обращения: 18.05.2012).