УДК 004.056.55

Электронная подпись и правовое регулирование ее использования в России и других странах

Бондаренко Владислав Витальевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Хильченко Лилия Нафисовна
Приамурский государственный университет имени Шолом-Алейхема
Старший преподаватель кафедры информационных систем, математики и методик обучения

Аннотация
Во всем мире наблюдается тенденция к переходу на электронный документооборот. Это в значительной степени позволит экономить время и деньги, а также обеспечит надежную защиту от подделок документов. К сожалению, на данный момент не существует единых норм и законов, которые бы регулировали вопросы по информационной безопасности во всем мире. В каждой стране присутствую свои отличия в этой сфере. В данной статье пойдет речь о правовых и организационных проблемах применения электронной подписи.
Ключевые слова: криптография, электронная подпись, информационная безопасность, симметричное шифрование, асимметричное шифрование, дешифрование, секретный ключ

Digital signature and legal regulation of its using in Russia and other countries

Bondarenko Vladislav Vitalievich
Sholom-Aleichem Priamursky State University
Student

Khilchenko Liliya Nafisovna
Sholom-Aleichem Priamursky State University
Senior lecturer of the Department of Information Systems, Mathematics and training methodic

Abstract
Nowadays, we see a trend towards the transition to a digital workflow around the world. This will save much more time and money, also become a guarantee of reliable protection against counterfeit documents. Unfortunately, there are no general rules and laws that could regulate information security problems at the

moment. Each country has its own differences in this domain. This article describes the legal and organizational problems of using a digital signature.

Keywords: cryptography, digital signature, information security, symmetric encryption, asymmetric encryption, decryption, secret key

Прежде чем приступить к обсуждению регулирующих и правовых норм в сфере информационной безопасности и электронной подписи необходимо дать определения основным понятиям.

Криптография – это наука о способах защиты информации, обеспечения конфиденциальности и целостности данных, а также проверки подлинности авторства. В современном мире в эпоху компьютерной техники защита информации подразумевает в первую очередь сохранение конфиденциальности цифровых (электронных) данных в виде файлов. С помощью специальных математических алгоритмов производят шифрование и дешифрование информации. В процессе шифрования исходный текст преобразуется в новый абсолютно неразборчивый и нечитаемый текст, который называется шифртекстом. В ходе дешифрования происходит обратный процесс в результате чего восстанавливается изначальный смысл и структура исходного текста. В обоих случаях используется секретный ключ. Ключ – это секретная информация, используемая криптографическими алгоритмами для шифрования и дешифрования данных, проверки электронной подписи и вычислении кодов аутентичности (MAC). Ключи для создания электронной подписи как правило выдаются удостоверяющими центрами или их доверенными представителями в виде сертификатов. Сертификат электронной подписи – это документ, который содержит ключ проверки вместе со всей необходимой информацией о владельце.

Электронная подпись или электронная цифровая подпись (в старом варианте) – это информация в электронном виде, которая шифруется при помощи криптографических алгоритмов и присоединяется к другой (подписываемой) информации для идентификации личности подписывающего человека. Подпись, которую мы обычно ставим, когда подписываем какой-либо документ, позволяет подтвердить наше согласие и удостовериться в нашей личности, после чего документ вступает в юридическую силу. Точно для такой же цели служит и электронная подпись, которая позволяет подписывать электронные документы, упрощая документооборот предприятий.

Человечество еще с давних времен пыталось шифровать информацию для безопасной передачи, чтобы она не смогла попасть не в те руки. Изобретали изощренные способы, которые основывались на написании сообщений с использованием специальных алфавитов, знаков, а также перестановок, например, широко известный шифр Цезаря. Ключом в данной ситуации мог выступать листок со значениями всех букв и знаков или же с указанием алгоритма перестановки. Причем, как правило, в те времена и ключ, и алгоритм были секретными.

Фактически алфавит любого естественного языка, тоже является шифром. Мы шифруем определенные понятия и мысли с помощью символов алфавита, составляя слова, словосочетания, предложения, и человек, не знающий языка или не умеющий читать, не сможет понять, о чем идет речь. Но все эти способы давно устарели и являются ненадежными – ключ можно легко украсть, и даже при его отсутствии грамотный лингвист, потратив какое-то количество времени, сможет взломать шифр. Поэтому раньше криптография была уделом лингвистов, сейчас же она является чисто математической дисциплиной, так как все современные алгоритмы основываются на математических формулах. Однажды математики обнаружили, что существуют такие математические уравнения типа $y = a * x$, где мы, зная x и подставляя его в уравнение, можем без проблем определить значение y, но если мы попытаемся провести обратный процесс с разложением y на множители, чтобы узнать x, то сделать это будет очень проблематично – потребуется много времени и вычислений. Первыми данную идею предложили Уитфилд Диффи, Мартин Хеллман и Ральф Меркле в 1976 году. Именно на этом явлении и построены все современные алгоритмы шифрования.

Существуют несколько видов шифрования. Исторически самым первым появилось симметричное шифрование. Оно характеризуется наличием секретного ключа, который должен быть у обеих сторон, передающих сообщения. Данный ключ представляет из себя небольшую последовательность чисел и используется как для шифрования, так и для дешифрования сообщений. Благодаря тому, что ключ действует в обе стороны, такой способ шифрования и получил название симметричного. Симметричное шифрование является довольно простым и самым быстрым способом, благодаря чему оно используется для шифрования больших объемов данных. Но есть один существенный минус – обе стороны должны владеть ключом, что уже само по себе недостаточно надежно, но, когда количество участников документооборота возрастает, идентифицировать с достаточной точностью принадлежность ключа определенной личности становится практически невозможным. Соответственно, такой тип шифрование не очень подходит для создания электронной подписи, так как должно быть явное соответствие между конкретным человеком и секретным ключом, чтобы мы могли точно сказать, что именно этот человек действительно подписал документ.

В конце 1970-х годов зародилось новое направление в криптографии – асимметричное шифрование. В данном шифровании существуют два вида ключа – открытый и закрытый. Открытый ключ доступен обеим сторонам и используется для шифрования сообщений или проверки подлинности подписи, а закрытый ключ находится только у одного человека и с его помощью производится дешифрование сообщений и подпись электронных документов. Таким образом получаем: один человек – один закрытый ключ. При этом открытый и закрытый ключи по определенному алгоритму

взаимосвязаны, но они не равны друг другу. Поэтому, например, для подделки подписи не удастся использовать открытый ключ. Но без минусов никак не обойтись. Процессы шифрования и дешифрования происходят намного медленнее, чем в симметричном шифровании, потому что ресурсов компьютера тратится значительно больше и поэтому использование асимметричного вида шифрования не оптимально для больших объемов данных, но достаточно для шифрования ключа и создания электронной подписи.

Третий метод шифрования позволяет избежать недостатков первых двух и использовать их достоинства. Здесь все просто – мы кодируем большие объемы данных, например документы, используя симметричное шифрование, а сам ключ - используя асимметричное шифрование. Таким образом получаем достаточно надежный и быстрый способ защиты информации, который в подавляющем большинстве случаев используется в наши дни.

Обзором методов шифрования занимался один из представителей компании «Электронные офисные системы» [4].

Существует множество профессиональных, давно функционирующих программных продуктов и стандартов для шифрования данных и создания электронной подписи, которые используют самые разнообразные алгоритмы и их комбинации. Таковыми являются PGP, S/MIME – самые популярные, а также TLS/SSL, IPSEC/IKE. В этих стандартах используются как симметричные алгоритмы – AES, Blowfish, CAST, DES, так и асимметричные – RSA, DSA, Elgamal, Diffie-Hellman, ECDSA. В результате одного из исследований был реализован алгоритм асимметричного шифрования RSA, который является одним из популярных стандартов шифрования в США, а также разработано программное обеспечение, которое было использовано при обучении студентов по дисциплине «Информационная безопасность» [1]. Более подробно об алгоритме RSA и особенностях его реализации рассказано его создателями [8].

Область применения электронной подписи достаточно широка. Вот самые распространенные сферы:

1. Электронный документооборот. Как правило электронная подпись часто используется для подписания документов в пределах какой-либо компании. При этом наличие электронной подписи является важным условием обмена документами, так как это дает гарантию их юридической силы.

2. Электронная отчетность для контролирующих органов. В нынешних условиях многим компаниям удобнее всего сдавать отчетные документы в электронном виде. Компания может выбрать любой удобный для себя способ: специализированное программное обеспечение, программы фирмы 1С, Федеральной налоговой службы, Фонда социального страхования.

3. Оказание государственных услуг в электронном виде. В системе gosuslugi.ru граждане имеет право заверять документы и заявления, а также получать подписанные письма о рассмотрении обращения. В России в этой

сфере используются стандарты электронной подписи (ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») и сертифицированные криптографические системы, например, «Aladdin e-Token ГОСТ», а также «КриптоПро CSP».

4. Электронные торги. При свершении сделок на специальных сайтах используется электронная подпись в качестве подтверждения заключения контракта.

5. Арбитражный суд. Для решения споров между компаниями документы, заверенные электронной подписью, также могут использоваться в качестве доказательства, как и бумажные аналоги.

6. Документооборот с физическими лицами. Здесь есть много возможностей для заключения любых договоров среди физических лиц, но к сожалению данная сфера слабо развита и редко используется.

Также эксперты по криптографии высказали свое мнение по юридической значимости электронной подписи и сфере ее применения [6].

Можно сделать вывод, что применение электронной подписи обладает рядом неоспоримых преимуществ. Главное преимущество заключается в том, что электронную подпись технически очень сложно подделать. Тем не менее возможность подделки существует с участием человеческих факторов: кража электронной подписи, создание фальшивых удостоверяющих центров. Поэтому крайне необходимо придерживаться всех требований закона об электронной подписи, использовать только сертифицированные средства для создания электронной подписи и надежно хранить свой закрытый ключ. Второе преимущество состоит в самой электронной форме передачи документов, что освобождает людей от пересылки материальных носителей. Третьим преимуществом, вытекающим из предыдущего, является то, что документы, скрепленные электронной подписью, передаются с очень высокой скоростью с помощью Интернета.

Тем не менее есть исследования, которые свидетельствуют о недостатках и проблемах использования электронной подписи [5, 9]. Одним из главных недостатков является то, что электронную подпись руководители компаний получают на свое имя и копируют ее своим сотрудникам, но при этом продолжают нести полную юридическую ответственности за совершенные действия с этой подписью. Препятствует широкому распространению электронной подписи несоответствие российского законодательства в этой сфере с международным, о чем речь пойдет немного дальше. Существует психологический барьер, который не могут преодолеть люди, чаще всего старшего возраста, и препятствующий переходу на новые технологии. В таких ситуациях могут помочь различные образовательные тренинги, на которые должен отправлять своих подопечных руководитель компании. Также еще одним недостатком является дороговизна такой

подписи. Зачастую средняя цена колеблется в пределах от 2 до 10 тысяч рублей.

Многих исследователей интересовали вопросы правового и организационного регулирования использования цифровой подписи в Российской Федерации [2-3]. Помимо этого, был проведен сравнительный анализ использования электронной подписи в России и за рубежом [7]. Первым законом, регулирующим возможности использования электронной подписи, которая на тот момент называлась «электронная цифровая подпись», стал Федеральный закон от 10 января 2002 г. № 1–ФЗ «Об электронной цифровой подписи». Данный закон внес большой вклад в обеспечение безопасности при взаимодействии органов власти между собой и различными коммерческими и некоммерческими организациями. Для осуществления электронного бизнеса и банкинга важным является возможность установления достоверности электронной цифровой подписи, которая определяется применением различных криптографических способов. Это и является основным направлением в криптографии.

На сегодняшний день в Российской Федерации приняты и существуют следующие основные нормативно-правовые акты, которые регулируют использование электронной подписи:

1. Гражданский кодекс РФ (ст. 160, 434, 847). В данных статьях говорится о возможности заключения договора с использованием электронной подписи в случаях и порядке, предусмотренных законом; дается определение электронному документу; признается возможность распоряжения денежными средствами на банковском счете путем удостоверения электронной подписи [10, 11].

2. Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011. Данный закон стал логическим продолжением и совершенствованием предыдущего Федерального закона от 10 января 2002 г. №1 – ФЗ «Об электронной цифровой подписи». Он регулирует применение электронной подписи при совершении гражданско-правовых сделок, оказании государственных и юридических услуг [12].

3. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 определяет основные принципы правового регулирования в сфере защиты информации, такие как свобода получения информации, ее достоверность, недопустимость сбора информации о частной жизни. Также в законе написано о том, что ни одно программное обеспечение не должно иметь приоритета в использовании, если только применение конкретного продукта в сфере государственных информационных систем не установлено федеральными законами. Законом гарантируется возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа [13].

4. Федеральный закон № 402-ФЗ «О бухгалтерском учете» от 06.12.2011. Данный закон позволяет составлять бухгалтерские отчетные документы не только на бумажных носителях, но и в виде электронного

документа, подписанного электронной подписью, а также устанавливает требования к электронному документообороту. Средства воспроизведения электронных документов и проверки электронных подписей подлежат хранению не менее пяти лет с момента последнего составления бухгалтерской отчетности [14].

5. Налоговый кодекс РФ (ст. 169). Этот закон предусматривает составление счетов-фактур в сфере товаров и услуг в электронной форме при взаимном согласии обеих сторон и наличии у них технических средств для обработки этих счетов-фактур [15].

Отдельно стоит обсудить Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011, который является основополагающим в сфере использования электронной подписи. Данный закон был направлен на устранение недостатков Федерального закона №1-ФЗ, вот некоторые из них: применение единственной сертифицированной технологии электронной подписи (асимметричного шифрования); не соответствие международным стандартам, таким как «технологическая нейтральность», свобода в выборе и использовании средств электронной подписи; отсутствие регулирования в сфере гражданско-правовых сделок; недопущение к использованию электронной подписи юридическими лицами.

В итоге Федеральный закон № 63-ФЗ привнес в законодательство РФ следующие принципы:

1. Возможность использовать технологию электронной подписи любого вида, если применение конкретной технологии в определенной сфере не предусмотрено федеральными законами или другими нормативно-правовыми актами.

2. Невозможность подтверждения электронной подписи и подписанного электронного документа, не имеющего юридической силы, если такая электронная подпись была сделана с использованием средств автоматического создания электронных подписей.

Федеральный закон № 63-ФЗ предполагает создание удостоверяющих центров, которые должны пройти государственную сертификацию. Такие центры занимаются созданием и выдачей сертификатов ключей проверки электронных подписей, устанавливают сроки их действия, аннулирует ранее выданные сертификаты, ведет реестр выданных и аннулированных сертификатов.

Также этот закон определяет несколько видов электронных подписей: простая, усиленная неквалифицированная и усиленная квалифицированная.

В случае, когда мы можем подтвердить факт формирования определенной личностью электронной подписи посредством паролей и кодов, электронная подпись будет называться простой.

Усиленная неквалифицированная электронная подпись – это электронная подпись, которая была получена в результате криптографического преобразования информации, позволяет идентифицировать личность человека, обнаружить внесения изменений в

электронный документ и создается с применением средств создания электронных подписей.

Усиленная квалифицированная электронная подпись обладает всеми признаками неквалифицированной подписи, а также указывает ключ проверки в квалифицированном сертификате и используются только те средства создания электронной подписи, которые соответствуют определенным требованиям.

Согласно закону электронный документ, подписанный простой или усиленной неквалифицированной электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью в случаях, установленных законодательством. Участники электронного взаимодействия обязаны обеспечивать секретность ключей и уведомлять удостоверяющий центр о нарушении конфиденциальности, а также не использовать ключ электронной подписи, если есть основания полагать, что он был украден.

Впервые законодательство, регулирующее использование электронной подписи, было принято в США в штате Юта в марте 1995 года, которое провозгласило следующие цели: создание единой правовой базы для деятельности органов сертификации и проверки электронных документов; повышение надежности использования электронной подписи и снижение ущерба от ее подделки; поддержка электронной коммерции. Вслед за штатом Юта подобные законы были приняты в штатах Калифорния, Флорида, Вашингтон.

В США электронная подпись выдается в виде сертификата так же, как и в России. В 1991 году там был предложен стандарт цифровой подписи, который в основном ориентировался на внедрение электронного документооборота в государственных органах. При этом предполагалось привлечение к этому стандарту частных организаций. Однако на тот момент использовались электронные подписи с симметричным шифрованием, что создавало некоторые неудобства в эксплуатации такого рода сетей.

Одной из особенностей американской системы в сфере электронного документооборота является наличие негосударственного регулирования электронных подписей. Так, например, в 1996 году была принята система рекомендаций, которая давала практические указания по использованию электронной подписи. В России тоже периодически проводятся форумы и конференции по данной тематике, хотя их значение в регулировании правового поля заметно меньше.

Существует несколько общемировых подходов к законодательству в сфере электронной подписи:

1. Прескриптивная модель. Впервые была разработана в США. Предлагает использование только одной определенной технологии, прошедшей аккредитацию и проверку на надежность. Только в таком случае электронная подпись признается действительной. Модель используется в Германии, Италии, Малайзии, а также какое-то время применялась и в России.

2. Минималистическая модель. Также была разработана в США. Данная модель предлагает большее количество свобод в выборе технологий и их уравнивание. При этом главную роль здесь выполняют судьи. Все это ведет к устранению барьеров на пути широкого внедрения электронного документооборота. В основном данную модель применяют в США и Канаде.

3. Гибридная модель. Модель была создана в ООН и старается объединить в себе предыдущие две. В целом любые электронные подписи признаются действительными, но существует список привилегированных технологий. Эта модель была закреплена в Директиве ЕС № 1999/93/ Европарламента и Совета «Об электронных подписях» от 13 декабря 1999 года и на данный момент используется в России.

Самым значимым международным документом по регулированию использования электронной подписи является Типовой закон ЮНСИТРАЛ об электронных подписях, который был принят 5 июля 2001 года на заседании сессии ЮНСИТРАЛ в Вене [16]. Данный закон был основан на гибридной модели и предложил новые стандарты оценки надежности электронной подписи, которые позволили компаниям заранее оценивать юридическую силу электронной подписи, не дожидаясь результатов экспертизы. ЮНСИТРАЛ является главным юридическим органом ООН, который занимается проведением реформ в области коммерческого права и модернизацией норм международной коммерческой деятельности.

Общемировые тенденции ведут к переходу от закрытого к открытому, но ограниченному типу документооборота. Закрытый тип подразумевает предварительное соглашение сторон и более жесткое контролирование, тогда как для открытого типа характерен свободный обмен ключами. Открытый, но ограниченный тип документооборота характеризуется наличием посредника между сторонами, роль которого должен играть удостоверяющий центр. Для осуществления такого перехода необходимо создание единого правового и экономического пространства, что и происходит сейчас в Европе.

В целом тенденции в развитии права использования электронной подписи и в России, и на международном уровне можно охарактеризовать положительно. Однако существуют определенные неточности и недостатки в законодательстве России, которые препятствуют широкому применению электронной подписи. Так, например, не совсем понятны определения усиленной и квалифицированной подписей, а также в чем состоят их отличия и какова область их применения. Еще одной проблемой является то, что не во всех случаях простая или неквалифицированная подпись является эквивалентной собственноручной. В России довольно слабо развито гражданское общество [17-21], что влечет за собой слабое регулирование вопросов по электронному документообороту со стороны общества. Поэтому необходимо, чтобы выработкой нововведений занималась не только власть, но и народ. Для этого было бы хорошо проводить больше различных семинаров и конференций с привлечением людей из властных структур. Также необходимо позаботиться о подготовке профессиональных кадров в сфере информационных технологий, которые зададут вектор дальнейшего

развития в этой сфере. Для осуществления всех этих задач потребуется ресурсы разного рода: информационные, научные, правовые, финансовые, кадровые, организационные. Принятие нового более совершенного закона об электронной подписи жизненно необходимо для развития информационного общества. Европа, как правило, является наиболее развитым и продвинутым регионом мира, где все инновации быстро воплощаются в жизнь. Россия не должна стоять в стороне, когда это касается каких-либо общемировых тенденций развития. Поэтому на сегодняшний день встает задача приблизить наше законодательство в сфере электронной подписи к общеевропейскому, а также начать воплощать самые последние мировые достижения в жизнь. Общие законы и стандарты позволят в значительной степени облегчить заключение договоров и со временем полностью перейти на электронный документооборот даже в сфере гражданских сделок, что избавит людей от работы с бумагами.

Библиографический список

1. Бондаренко В.В., Козич В.Г., Баженов Р.И. Реализация алгоритма асимметричного шифрования RSA // Постулат. 2016. № 1 (1). С. 9.
2. Тарасов А.М. Криптография и электронная цифровая подпись: правовые и организационные аспекты // Вопросы теории и практики. 2011. №22. С. 9-19.
3. Задорожная И.В. Правовые аспекты использования электронной цифровой подписи в компьютерных сетях банковских организаций // Перспективы развития информационных технологий. 2012. №7. С. 235-240.
4. Электронная цифровая подпись для чайников: с чем ее есть, и как не подавиться. Часть 3 // Хабрахабр URL: https://habrahabr.ru/post/98323/ (дата обращения: 04.12.2017).
5. Электронная подпись: практическое использование на предприятии программного продукта CyberSafe Enterprise. Часть первая // Хабрахабр URL: https://habrahabr.ru/company/cybersafe/blog/247019/ (дата обращения: 04.12.2017).
6. Просто об электронной подписи // ECM-Journal URL: https://ecm-journal.ru/e-sign (дата обращения: 04.12.2017).
7. Сравнительный анализ использования ЭП в России и за рубежом // Zakon URL: https://zakon.ru/blog/2013/3/29/sravnitelnyj_analiz_ispolzovaniya_ep_v_rossii_i_za_rubezhom (дата обращения: 04.12.2017).
8. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Volume 21 Issue 2.
9. Худкина Е.А., Долгова Т.Г. Проблемы использования электронно-цифровой подписи на электронных торгах // Актуальные проблемы авиации и космонавтики. 2014. №10. С.397-398
10. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994

N 51-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 06.08.2017) // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 06.12.2017).
11. "Гражданский кодекс Российской Федерации (часть вторая)" от 26.01.1996 N 14-ФЗ (ред. от 28.03.2017) // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_9027/ (дата обращения: 06.12.2017).
12. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 06.12.2017).
13. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 06.12.2017).
14. Федеральный закон от 06.12.2011 N 402-ФЗ (ред. от 18.07.2017) "О бухгалтерском учете" // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_122855/ (дата обращения: 06.12.2017).
15. Налоговый кодекс Российской Федерации часть 2 (НК РФ ч.2) // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_28165/ (дата обращения: 06.12.2017).
16. Типовой закон ЮНСИТРАЛ об электронных подписях (2001 год) // ЮНСИТРАЛ URL: http://www.uncitral.org/uncitral/ru/uncitral_texts/electronic_commerce/2001Model_signatures.html (дата обращения: 06.12.2017).
17. Бакирова С.К. Россия: где гражданское общество? // Вестник магистратуры. 2017. №11-2 (74). С. 91-94.
18. Зорько И.С. Политическая партия «Справедливая Россия» как субъект оппозиции и гражданского общества // Государственное и муниципальное управление. Ученые записки СКАГС. 2013. №4. С. 222-226.
19. Бойков В.Э., Тощенко Ж.Т., Егоров В.К., Левашов В.К., Жук И.Д., Туманов С.В., Шабров О.Ф., Яковлев И.Г., Марченко Г.И., Патрушев В.И., Леденева В.Ю., Митрошенков О.А. Состоялось ли гражданское общество в России (материалы «круглого стола») // Социология власти. 2006. №4. С. 73-105.
20. Что происходит с гражданским обществом в России? // Радио Свобода URL: https://www.svoboda.org/a/2137680.html (дата обращения: 08.12.2017).
21. Косорукова О.А. Существует ли гражданское общество в России? // Социально-политические науки. 2013. №1. С.85-86