ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ВНЕДРЕНИЯ СТОЙКИХ ЧАСТНЫХ КРИПТОСИСТЕМ

*Гриднев В. А., Володин И. С., Желудкова А. М.**

***Ключевые слова**: правовое регулирование, защита информации, права человека, национальная безопасность, стойкое шифрование, честная криптосистема, шифрование с депонированными ключами, пороговые схемы разделения секрета, контроль аутентичности теней.*

Аннотация.

Цель работы: исследование задачи правового регулирования отношений в области стойкого шифрования личной информации граждан в различных странах и способов ее решения.

Метод: системный организационно-правовой анализ влияния нормативно-правового обеспечения на развитие частных криптографических систем.

Результаты: рассмотрена оценка степени влияния нормативных правовых документов и законодательных актов на развитие криптографических систем для частного использования; обоснована наиболее перспективная технология развития систем депонированного шифрования личной информации граждан, основанная на реализации пороговой схемы разделения секрета с возможностью контроля аутентичности теней ключа шифрования.

DOI:10.21681/1994-1404-1-51-60

Введение

Вплоть до 90-х годов XX в. стойкое компьютерное шифрование использовалось по большей части национальными правительствами и крупными компаниями. Однако в июне 1991 г. американский программист Фил Циммерман, убежденный в необходимости защиты электронной почты от перехвата, открыл шифрование онлайн-коммуникаций частным лицам, поместив разработанную им программу *PGP* на электронной доске объявлений *Usenet*. С этого момента доступ к устойчивой криптографии получил любой желающий, и вокруг права на шифрование разгорелась дискуссия, которая фактически свелась к вопросу о том, должны ли правительства законодательно запретить использование стойкой криптографии своим гражданам или же нет. Споры не утихают по сей день[1] [1].

Убежденность правозащитников в необходимости доступа частных лиц к шифрованию основывается на ст. 12 Всеобщей декларации прав человека 1948 г.[2]: *«Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту от такого вмешательства или таких посягательств».* Аналогичные нормы закреплены в п. 1 ст. 8 Конвенции о защите прав человека и основных свобод 1950 г., ст. 17 Международного пакта о гражданских и политических правах 1966 г. и иных международных договорах.

Но практически в любом государстве, в том числе и в России, есть серьезные основания полагать, что широкое использование криптографии может содейство-

[1] Advances in Cryptology — CRYPTO '92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992. Proceedings [Текст]. Springer, 2003. 593 p.; Правовое регулирование шифрования онлайн-коммуникаций. URL https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

[2] Всеобщая декларация прав человека. М.: Права человека, 1996. — 16 с.

* ***Гриднев Виктор Алексеевич,*** *кандидат технических наук, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: vikadres@yandex.ru

Володин Иван Сергеевич, *студент Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: ivolodin98@gmail.com

Желудкова Анастасия Михайловна, *студент Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*
E-mail: anasanutasia@gmail.com

вать преступным и террористическим организациям. Поэтому во многих законах прописано, чтобы надлежащее государственное учреждение при обстоятельствах, разрешенных законом, в рамках своей работы могло получить открытый текст любого шифрованного сообщения. В настоящее время это требование выражается в принуждении граждан к использованию слабых криптосистем, т. е. таких, которые надлежащие органы власти (но, естественно, и все желающие) могут взломать с умеренными усилиями, либо к раскрытию секретного ключа шифрования органам власти.

Приведем цитату из «Книги шифров» Саймона Сингха, в которой автор приводит аналогию, сформулированную Роном Ривестоном, одним из создателей алгоритма шифрования *RSA*: «*Плохо без разбора запрещать технологию только потому, что некоторые преступники могут использовать ее в своих целях. Так, любой гражданин США может свободно купить пару перчаток, даже при том, что ими мог бы воспользоваться грабитель, чтобы обчистить дом, не оставив отпечатков пальцев. Криптография — это средство для защиты данных, точно так же, как перчатки — средство для защиты рук. Криптография защищает данные от хакеров, корпоративных шпионов и мошенников, в то время как перчатки предохраняют руки от порезов, царапин, жары, холода, инфекции. Первая может воспрепятствовать ФБР прослушивать телефонные разговоры, а вторые — помешают ФБР найти отпечатки пальцев. И криптография, и перчатки — они дешевле пареной репы и есть везде*» [10].

В Российском законодательстве пока еще не отражена такая тема, как собственноручная передача ключей шифрования спецслужбам со стороны граждан и организаций [6]. Но эта идея активно обсуждается. Она не вызывает недовольства у производителей — им не придётся вносить никаких доработок в свои продукты. Проект не очень-то масштабируем[3], но это не помешало некоторым государствам вместо депонирования ключей внедрить способ законного получения ключей от самих пользователей по требованию правоохранительных органов. В противном случае гражданам грозит уголовная ответственность за отказ в помощи следствию. В России таких норм на данный момент нет.

Законодательство и криптография

В России данная тема пока не актуальна, ключи у нас сейчас требуют только от операторов распространения информации, зарегистрированных в специальном реестре ФСБ, а простые граждане пока ограничены только Законом о лицензировании отдельных видов деятельности[4]. На рис. 1 приведены примеры государств, которые ввели у себя законы о передаче ключей шифрования (по данным английской Википедии, ссылающейся на законодательные акты соответствующих стран).

В Латвии в ноябре 2015 г. стало известно о готовящихся поправках в Уголовный кодекс, которые могут ввести наказание за использование программного обеспечения, препятствующего работе спецслужб[5].

Франция, посмотрев на предыдущий опыт США, попыталась в конце 20 в. внедрить у себя систему депонирования ключей. Премьер-министр Жоспен выразил желание внедрить данную систему, но уже через пару месяцев все работы по этому вопросу были прекращены. Министр внутренних дел Франции Бернар Казнев, ссылаясь на террористическую опасность, выступил за ограничение коммуникаций, защищенных *сквозным (оконченным)* шифрованием[6].

Йемен выступил с заявлением о своей собственной системе депонирования в 1997 г., правда, спустя год был объявлен перенос разработок на более дальний срок и по факту проект был заморожен [11].

В Великобритании с 2000 г. действует Акт «О правовом регулировании следственной деятельности» (*Regulation of Investigatory Powers Act* 2000), обязывающий пользователей систем шифрования по требованию властей предоставлять необходимые для расшифровки информации ключи и пароли. Отказ выполнить эти требования влечет за собой уголовное преследование[7].

В 2014–2016 гг. дискуссия о праве на шифрование и анонимность в Интернете достигла международного уровня. Проанализировав особенности и мотивы использования технологий шифрования в контексте основных прав человека, ООН признала анонимность в Интернете необходимым условием осуществления прав на свободу слова в цифровую эпоху[8].

В докладе Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея[9] дается оценка и интерпретация правам пользователей на шифрование в контексте основных прав и свобод человека, гарантируемых Международным пактом о гражданских и политических правах 1966 г. Основные его тезисы имеют принципиальное значение для понимания правового статуса шифрования в цифровой век.

---

[3] Из-за различий в законодательствах государств проблематично обеспечить широкое применение разработанного прикладного программного обеспечения, что неизбежно приводит к его удорожанию.

[4] Федеральный закон РФ от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» СПС «КонсультантПлюс».

[5] Сильная криптография. URL: https://ru.qaz.wiki/wiki/Strong_crypto-graphy (дата обращения 25.10.2020).

[6] Там же.

[7] History of cryptography. URL: https://en.wikipedia.org/wiki/History_of_ cryptography (дата обращения 11.10.2020).

[8] Правовое регулирование шифрования онлайн-коммуникаций. URL: https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

[9] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея 22 мая 2015 г. №A/HRC/29/32. URL: https://undocs.org/ru/A/HRC/29/32 (дата обращения 18.10.2020).

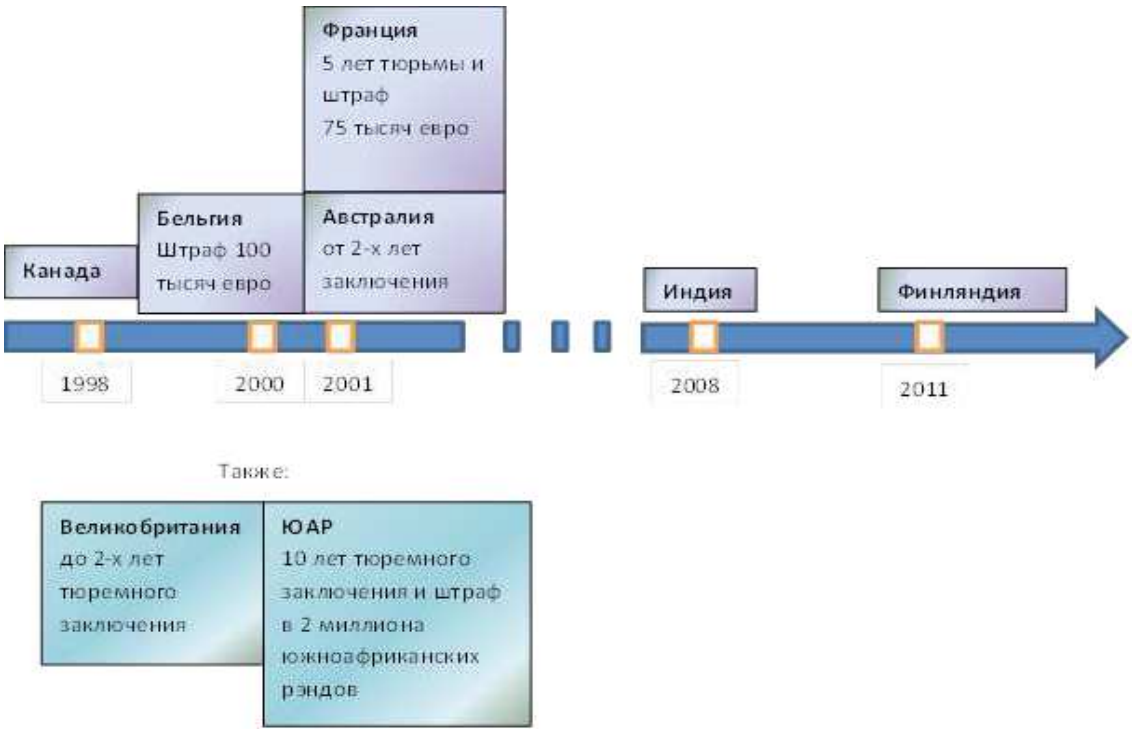

Рис. 1. Даты принятия законов и наказания за их несоблюдение

Сегодня в законах лишь некоторых стран официально содержатся статьи, регулирующие депонирование ключей. В Испании требуют разделять ключи для телекоммуникаций еще с 1998 г., но система так и не была принята для повсеместного использования. Великобритания в течение нескольких лет пыталась продвинуть политику, согласно которой национальные *удостоверяющие центры* могли получить соответствующую лицензию на работу только при условии получения приватных ключей у граждан. В конечном итоге от данной политики и в Великобритании тоже отказались.

В настоящее время в США нет никаких законов, обязывающих американских производителей внедрять какие-либо лазейки в подсистемы шифрования своих продуктов, так как это напрямую нарушает Пятую поправку к американской Конституции. Все вопросы по данной теме регулируются через суд, и результат всегда различается — некоторых принуждают предоставлять ключи, некоторых нет. Хотя в частном порядке такие системы разрабатывались, но не получили широкой огласки.

Итак, многие страны, не имея возможности требовать разделения ключей и не имея собственных разработчиков средств шифрования и телекоммуникационных средств, использующих криптографическую защиту, которые могли бы внедрить системы для восстановления ключей или иные лазейки, требуют от граждан и бизнеса предоставлять ключи шифрования по требованию государства[10].

Россия только встаёт на этот путь (началом можно считать закон, который в народе назвали по имени одного из инициаторов его принятия: «Пакет Яровой») и такие альтернативы тревожат многих активных граждан, считающих, что неприкосновенность частной жизни должна быть важнее национальной безопасности и задач правоохранительных органов.

Криптосистемы с депонированием ключей

Чтобы граждане могли воспользоваться всеми преимуществами сильной криптографии, совершенно не обязательно становиться на путь криптоанархии. Есть очень перспективная альтернатива — шифрование с депонированными криптоключами (или *депонированное шифрование*)[11] [9, 13]. Суть такого шифрования заключается в соединении преимуществ сильного шифрования и аварийного дешифрования. Стандартный ключ не должен быть тем ключом, который используется при нормальном дешифровании, однако он должен обеспечивать доступ к такому ключу по решению суда. Ключ дешифрования разделяется на части и находится у доверенных лиц, которыми могут быть государственные службы, суд, нотариусы или даже частные компании. Организации, являющиеся агентами по депонированию, могут также иметь собственные средства и ключи для аварийного дешифрования. Правоохранительные органы для получения доступа к зашифрован-

[10] Сильная криптография. URL: https://ru.qaz.wiki/wiki/Strong_cryptography (дата обращения 25.10.2020).

[11] Micali S. Fair Public-Key Cryptosystems, «Advancesin Cryptology CRYPTO'92» Proceedings, Springer-Verlag, 1993, pp. 113-138.

ной информации должны обратиться в суд и получить ордер на получение ключа для дешифровани.

Высказанная выше идея не нова. Впервые вопрос о депонировании ключей был поднят в США в 1992 г. Эта система позволяла бы спецслужбам получать доступ к защищенным перепискам граждан для проведения расследования. Изначально было задумано, что такую возможность будут автоматически встраивать во все устройства шифрования, разрабатываемые в то время в США. Альтернативным решением была идея встраивать в телекоммуникационные средства специальные потайные ходы, которые позволяли бы расшифровать данные переписки даже без знания ключа.

Администрация президента Клинтона вынесла предложение использовать специально спроектированный при сотрудничестве *NSA* и *NIST* чип *Clipper*, который мог использовать новый на то время криптографический алгоритм *Skipjack*, созданный для замены *DES*[12] [2]. Ключ в 80 бит у *Skipjack* считался более надежным, чем 56 бит у *DES*, однако для восстановления данных государство обязывало хранить все ключи в специальной закрытой базе данных. Технология разделения ключа была вшита в чип по умолчанию, и производители, которые будут встраивать чип в свои устройства, должны будут дополнительно передавать ключи для дешифрования в соответствующие органы. Для того чтобы продвинуть чип *Clipper* на рынке, администрация Клинтона планировала оснастить все телефоны и компьютеры, используемые в государственных учреждениях, этим чипом, создав большой госзаказ для снижения конечной стоимости продукта.

Несмотря на принятые меры, инициатива администрации президента по внедрению чипа *Clipper* предсказуемо встретила, как и следовало ожидать, сильное недовольство со стороны американского бизнеса и общественности, которое сопровождалось тремя ключевыми тезисами:

- использование чипа *Clipper* приводит к нарушению конституционных прав граждан на тайну переписки и личной жизни;
- защищенность базы данных с ключами для дешифрования не гарантирует невозможность её взлома и утечки ключей [4];

алгоритм *Skipjack* был секретным и частные эксперты не могли провести анализ на предмет уязвимостей и незадокументированных возможностей. У экспертов возникли явные подозрения, что кроме базы данных ключей алгоритм содержит дополнительные лазейки, которые позволили бы расшифровывать данные даже без знания ключа[13].

В конечном итоге инициатива с чипом *Clipper* провалилась, но провал не смог остановить администрацию Клинтона и в 1995 г. она выпустила обновленный план *Clipper* II. В новой редакции программы *Clipper* допускалось хранение баз ключей у частных независимых организаций, к которым сотрудники спецслужб все равно могли получить полный доступ.

В 1996 г. 20 мая был выпущен документ под названием *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, который критики без промедления прозвали *Clipper* III. Этот проект выделялся от предыдущих большей интеллектуальностью — в нём не использовались никакие дополнительные чипы в устройствах, идея которых была изначально мёртвой. Вместо этого была предложена новая система управления ключами, которая давала простым гражданам и частному бизнесу легкий способ подтверждения сертификатов открытых ключей, так нужных в электронной коммерции. По сути, речь шла о *федеральном удостоверяющем центре*, целью которого стало бы хранение ключей пользователей в базе данных. Эксперты полностью раскритиковали и эту идею, как и две предыдущие [1].

В 1996 г. 1 октября администрация Клинтона снова выступила с новой инициативой, которая должна была вступить в силу с 1 января 1997 г. Планировалось передать ответственность за экспорт криптографии из Министерства юстиции в Министерство торговли. Длина ключей, которые были разрешены к экспорту без ограничений, была увеличена с 40 до 56 *бит*. Кроме того, производители получили бы право экспортировать и более сильные криптографические средства, получая специальное разрешение в Министерстве торговли. Однако на деле снова было одно очень отталкивающее ограничение — разрешение на экспорт сопровождалось требованием встроить в механизмы шифрования средство для восстановления ключей, которое позволило бы спецслужбам снова получить полный доступ к защищённым данным. Как и следовало ожидать, данная инициатива была опять встречена очень негативными отзывами со стороны производителей, и администрация Клинтона, наконец, устав бороться с противниками усиления национальной безопасности, передала все полномочия по всем вопросам, связанным с криптографией, в Конгресс[14].

Прошло немного времени, и на рассмотрение в Конгресс был выдвинут проект закона *Security and Freedom Through Encryption Act* (*SAFE*), который установил некоторые спорные с точки зрения правозащитников положения:

- запрещено требовать от американских производителей встраивать в свои продукты в механизмы для разделения или восстановления ключа;

[12] McCullough B. The NSA tried this before — what the 90s debate over the clipper chip can teach us about digital privacy. URL: http://www.internethistorypodcast.com /2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-de-bates/ (дата обращения: 10.10.2020); Ловцов Д. А. Контроль и защита информации в АСУ. М.: ВА им. Петра Великого, 1991. 172 с.

[13] Там же.

[14] Правовое регулирование шифрования онлайн-коммуникаций. URL: https://digitalrights.center/blog/pravovoe-regulirovanie-shifrovaniya-onlayn-kommunikatsiy/ (дата обращения 10.12.2020).

- на территории США разрешено производство, распространение и использование любых средств шифрования, независимо от используемых алгоритмов и размера ключей (по принципу «бизнес-выбора» [3]);
- разрешено производить на экспорт криптографические средства, если на международном рынке присутствует схожий продукт;
- запрещено использовать средства шифрования для незаконных целей.

Интересный факт: в одну из версий данного закона предлагали включить пункт, гласящий, что любое импортируемое в США криптографическое оборудование или программное обеспечение должно иметь возможность восстановления ключей шифрования, но данная норма, естественно, не была принята. Сегодня в США на импортированные средства шифрования нет никаких ограничений.

Законопроект *SAFE* рассматривался в Конгрессе около 2 лет, но так и не был принят. Впоследствии в Конгресс было внесено большое число новых законов, которые пытались узаконить требования по вопросам применения и экспорта шифровальных средств, среди них:

- *The Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act;*
- *The Electronic Rights for the 21stCentury Act;*
- *The Encryption for the National Interest Act;*
- *The Secure Public Networks Act* и др.

Но ни один из разработанных законопроектов так и не был подписан Президентом США. С 2001 г. ни один законопроект на данную тематику так и не был вынесен на обсуждение в Конгресс.

В 1998 г. в регламент экспорта шифровальных средств были внесены некоторые исправления, которые установили точный список стран и индустрий, в которые можно экспортировать американские шифровальные средства без ограничений, в иных случаях Министерство торговли США должно было выдавать специальное разрешение. Требования к системам депонирования ключей стали ниже, а позднее, в 2000 г., и вовсе были сняты. Все это было связано не только с препятствиями, с которыми столкнулась администрация Клинтона, но и с подписанием в декабре 1996 г. Вассенарских (Нидерланды, г. Вассенар) соглашений[15]. Принятые договоренности, по сути, полностью запретили разделение ключей для дешифрования. США попытались получить некоторые льготы и послабления на экспорт средств, отнесенных к технологиям, предназначенным для военного и гражданского использования, но им это не удалось. В итоге США пришлось полностью отказаться от своих планов, потому что эксперты в рабочей группе не смогли прийти к единому соглашению.

[15] Вассенарские договоренности (33 страны) по экспортному контролю за обычными вооружениями, товарами и технологиями двойного назначения. URL: https://www.wassenaar. org/ru/ (дата обращения 18.12.2020).

Возможные перспективы частной криптографии

Идея возможности использования сильной криптографии в частных целях впервые была предложена в 1993 г. Сильвио Микали, американским ученым в области теории вычислительных систем, лауреатом премии Геделя 1993 г. и премии Тьюринга 2012 г. Свою идею он назвал *"честной криптосистемой"*. Она заключается в создании криптосистемы, которая может обеспечивать хороший баланс между потребностями правительства и потребностями граждан. Честные криптосистемы гарантируют [4] две вещи:

1. конфиденциальность законопослушного пользователя не может быть нарушена;
2. злоумышленники не могут рассчитывать на конфиденциальность[16].

В честной криптосистеме есть фиксированное количество заранее назначенных доверенных лиц и произвольное количество пользователей. Доверенными лицами могут быть федеральные судьи, нотариусы, а также различные общественные организации, такие как группа гражданских прав, или компьютеры, контролируемые ими и оснащенные прикладным программным обеспечением, специально созданным для этой цели. Доверенные лица вместе с отдельными пользователями и центром распределения ключей играют решающую роль в уровне доверия честным криптосистемам[17].

Данная схема может быть усовершенствована использованием пороговой схемы разделения секрета, позволяющей восстановить разделенный секрет по k из n частей (теней). Пользователь может создать свой собственный закрытый ключ и распределить его части среди n доверенных лиц. Ни один из них не может восстановить закрытый ключ. Однако каждый может проверить аутентичность своей части (тени) закрытого ключа[18] [13].

Если судебные власти разрешат подслушивание, соответствующие правоохранительные органы смогут воспользоваться постановлением суда для того, чтобы любые k из n доверенных лиц выдали свои тени ключа. Собрав нужное количество частей, власти восстановят закрытый ключ и смогут подслушивать линии связи пользователя. С другой стороны, чтобы получить возможность восстановить ключ пользователя и нарушить тайну личности, злоумышленнику придется подкупить нужное количество доверенных лиц [9].

Для конкретности рассмотрим принципы построения пороговой схемы разделения секрета два из трех: <2; 3>.

[16] Micali S. Fair Public-Key Cryptosystems, «Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 113-138.

[17] Там же.

[18] Shamir A. How to share a secret [Электронный ресурс] / Communications of the ACM. 1979. Vol. 22, No. 11. URL: https://dl.acm.org/doi/10.1145/359168.359176 (дата обращения 12.11.2020).

Программный модуль вычисления теней создает 3 тени секретного ключа пользователя для последующей их передачи нотариусам и формирует электронную подпись пользователя к каждой тени. Разделение производится таким образом, что:

– для восстановления секрета достаточно двух теней;
– одна сторона не сможет получить никакой информации о секрете.

Такое разделение осуществляется с помощью схемы интерполяционных полиномов Лагранжа (схемы разделения секрета Шамира или схемы Шамира) — схемы разделения секрета, широко используемой в криптографии [13].

Для интерполяции многочлена степени k–1 требуется k точек. Основная идея данной схемы состоит в том, что интерполяция невозможна, если известно меньшее число точек[19]. Например, многочлен степени 1 представляется графически как прямая линия на плоскости и для его восстановления требуется знать значение функции в двух точках (рис. 2). Искомым секретом в данном случае является значение полинома в точке $x = 0$.

Необходимо разделить секрет M между тремя сторонами таким образом, чтобы любые два участника могли восстановить секрет, т. е. нужно реализовать <2; 3>-пороговую схему.

Выберем некоторое простое число $p > M$. Это число можно открыто сообщать всем участникам. Оно задает конечное поле размера p. Над этим полем построим линейное уравнение, т. е. случайно выберем все коэффициенты многочлена, кроме M:

$$F(x) = (a_1 \cdot x + M) \bmod p. \quad (1)$$

В этом многочлене M — это разделяемый секрет; a_1 — некоторое случайное число, которое нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

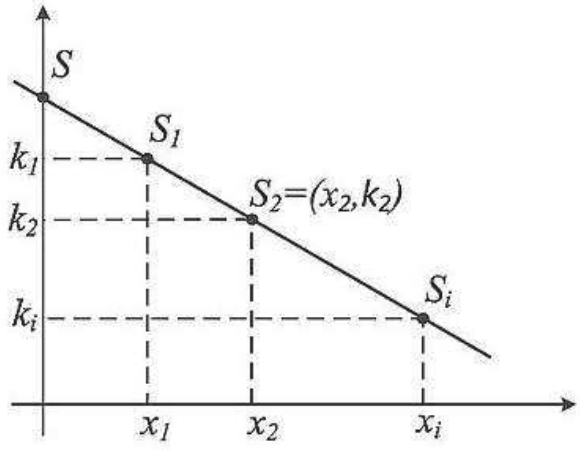

Рис. 2. Графическое представление разделения секрета <2; 3>

Теперь вычисляем «тени» — значения построенного выше многочлена в трех различных точках, причем $x \neq 0$:

$$\begin{aligned} k_1 &= F(1) = (a_1 \cdot 1 + M) \bmod p; \\ k_2 &= F(2) = (a_1 \cdot 2 + M) \bmod p; \\ k_3 &= F(3) = (a_1 \cdot 3 + M) \bmod p. \end{aligned} \quad (2)$$

Аргументы многочлена (номера теней) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдается доля секрета — тень k_i вместе с номером i. Помимо этого, всем сторонам сообщается степень k–1 многочлена (1) и размер поля p. При этом число p должно быть простым и меньше основного секрета M. Случайный коэффициент a_1 и сам секрет M «забываются»[20].

Для того чтобы нотариус впоследствии мог удостовериться в аутентичности доверенной ему тени, после ее формирования происходит вычисление электронной подписи к этой тени с использованием закрытого ключа пользователя, выдаваемого удостоверяющим центром. Кроме того, использование электронной подписи предоставляет возможность обеспечить следующие свойства при передаче или хранении в системе подписанной тени:

– осуществление контроля *целостности* подписанной тени;
– доказательное подтверждение авторства лиц, подписавших сообщение;
– защита тени от возможной модификации или подмены.

Схематическое представление подписанного сообщения показано на рис. 3 [10].

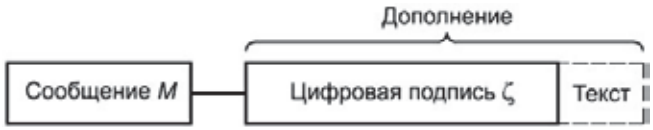

Рис. 3. Структура подписанного сообщения

Под сообщением здесь понимается одна из теней ключа шифрования. Цифровая подпись — это число фиксированной длины, однозначно зависящее от подписываемого сообщения (тени ключа шифрования) и секретного ключа субъекта подписи. Поле «Текст», показанное на рис. 3 и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени [10].

В качестве алгоритма вычисления электронной подписи можно использовать алгоритм ГОСТ Р 34.10-2012[21].

[19] Shamir A. How to share a secret [Электронный ресурс] / Communications of the ACM. 1979. Vol. 22, No. 11. URL: https://dl.acm.org/doi/10.1145/359168.359176 (дата обращения 12.11.2020)..

[20] Там же.

[21] ГОСТ 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции [5, 7]. Алгоритм вычисления хэш-функции установлен ГОСТ Р 34.11-2012[22].

Сгенерированная тень вместе с электронной подписью пользователя записывается на съемный носитель, предъявляемый нотариусу, либо пересылается доверенным лицам по защищенному каналу связи, а затем гарантированно стирается из памяти устройства.

Для того чтобы нотариус мог удостовериться в аутентичности вручаемой ему тени ключа, нужно специальное прикладное программное обеспечение. Назовем его *модулем проверки корректности теней*.

Так как модуль генерации ключа шифрования совместно с модулем вычисления теней составляют один программно-аппаратный комплекс, вероятность ошибки которого крайне мала, проверка нужна для того, чтобы удостовериться в целостности и аутентичности тени ключа. Это позволяет, с одной стороны, исключить возможность подмены тени, вручаемой нотариусу, а с другой стороны — проверить аутентичность тени, получаемой представителем спецслужбы государства у нотариуса.

Модуль восстановления ключа должен быть в составе информационной системы спецслужб. Он используется, когда нужно восстановить секретный ключ пользователя с разрешения суда. При этом над любыми двумя из трех теней выполняется преобразование, результатом которого является восстановленный ключ.

Зная координаты k (двух) различных точек многочлена, можно восстановить многочлен, включая и свободный член — разделяемый секрет. Для этого можно использовать интерполяционный полином Лагранжа:

$$F(x) = \sum_i l_i(x) y_i (mod\ p),$$
$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} (mod\ p). \quad (3)$$

Обозначения переменных в выражении (3) аналогичны обозначениям в выражении (1).

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных k–1 теней (в рассматриваемом случае это будет одна тень) оценивается как p^{-1}. То есть в результате интерполяции по k–1 точкам секретом может быть любой элемент поля с равной вероятностью. При этом попытка полного перебора всех возможных теней не позволит злоумышленникам получить дополнительную информацию о секрете.

Перед непосредственным восстановлением ключа должны быть проверены электронные подписи теней, полученных от нотариусов.

Общая схема взаимодействия субъектов в рассматриваемой системе может быть такой, как описано ниже. Модуль генерации ключа шифрования и модуль вычисления теней составляют один программно-аппаратный комплекс. Он должен быть расположен в защищенном помещении в пределах контролируемой зоны *центра распределения ключей* [3].

Если пользователь желает использовать честную криптосистему, он должен обратиться в центр распределения ключей и подать заявку, указав в ней свои персональные данные (ФИО, серию и номер паспорта, номер телефона), и дожидаться ответа. Центр распределения ключей вносит эту информацию в базу данных, осуществляет выбор нотариусов и извещает участников (пользователя и нотариусов) о времени выдачи ключа шифрования и соответствующих теней. Все это можно сделать с помощью телекоммуникаций [8, 12]. Обеспечение безопасности (конфиденциальности, целостности и доступности) [3] передачи ключа и теней выходит за рамки данной статьи.

Стоит заметить, что данные нотариусов, как и пользователей, вносятся в базу данных центра распределения ключей, и после генерации ключа и распределения теней идентификаторы нотариусов будут включены в запись о соответствующем вручении ключа. Таким образом, в случае разрешения судом прослушивания линий связи пользователя, правоохранительные органы будут знать, у каких доверенных лиц находятся нужные тени.

Пользователь теперь может использовать надежный ключ шифрования, полученный в центре распределения ключей, а нотариусы будут хранить тени этого ключа в секрете.

Нотариус в любой момент может проверить электронную подпись тени, чтобы убедиться в том, что тень сгенерирована конкретным центром распределения ключей и не была модифицирована с момента ее создания. Для этого ему нужно знать открытый ключ центра распределения ключей и иметь программное обеспечение, позволяющее выполнять проверку электронной подписи. Это программное обеспечение представляет собой модуль проверки корректности тени.

В случае разрешения прослушивания судом правоохранительные органы смогут обратиться в центр распределения ключей и выяснить контактные данные нотариусов, которые хранят тени секретного ключа пользователя. Получение хотя бы двух из трех теней позволяет восстановить секрет с помощью модуля восстановления ключа, который также представляет собой специальное программное обеспечение.

Полученный в результате восстановления ключ дает возможность либо успешно расшифровать переписку пользователя, либо уличить его в использовании другого ключа, если электронные подписи всех теней проходят проверку подлинности. Если электронная подпись тени, полученной у нотариуса, не проходит проверку, значит, целостность тени была нарушена и поскольку тень находится у нотариуса, он несет ответственность за ее сохранность.

[22] ГОСТ 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

Очевидных технических проблем реализации предложенной системы нет. Но у каждого пользователя существует принципиальная возможность, получив депонированный ключ шифрования, для реального информационного обмена использовать иной ключ. Поэтому законодательством должна быть предусмотрена строгая ответственность за такого рода правонарушения.

Заключение

Таким образом, широкое внедрение стойких криптосистем для защиты тайны частной жизни граждан, гарантированной Конституцией, в России, как и в других странах, сопряжено со многими трудностями, связанными прежде всего с обеспечением национальной безопасности. Наиболее перспективной, с учётом опыта других стран, представляется технология *депонированного шифрования*, дополненная пороговой схемой разделения секрета (схема Шамира). Но это, в свою очередь, требует разработки надёжных технических механизмов и юридических процедур, не позволяющих пользователям и доверенным органам подменять тени реальных ключей шифрования ложными файлами, которые не позволят соответствующим государственным органам восстановить реальные ключи даже после соответствующего решения суда. Такие механизмы и процедуры возможно установить в результате:

- принятия Федерального Закона РФ «О защите частной жизни граждан в информационном обществе»;
- внесения в КоАП РФ и в УК РФ изменений и дополнений, предусматривающих ответственность за недобросовестные действия при использовании депонированных ключей шифрования;
- издания Постановления Правительства РФ «О депонировании ключей шифрования личной информации граждан»;
- издания руководящего документа ФСБ России «Методика контроля корректности депонированных ключей шифрования личной информации граждан»;
- разработки, государственной сертификации и регистрации в Федеральном реестре прикладного программного обеспечения ЭВМ, позволяющего генерировать ключи шифрования и их тени, проверять аутентичность теней и восстанавливать ключи по нескольким теням из фиксированного множества (предпочтительно реализовать пороговую схему «два из трёх»).

К настоящему времени на кафедре информационных систем и защиты информации ФГБОУ ВО «Тамбовский государственный технический университет» разработано прикладное программное обеспечение ЭВМ, реализующее различные пороговые схемы разделения секрета.

Весь информационный обмен между субъектами взаимоотношений в данной системе можно реализовать в электронной форме, что неизбежно потребует принятия мер по обеспечению безопасности информации, передаваемой по каналам связи.

Литература

1. Алексеев В. В., Емельянов Е. В., Кастерин Д. А., Стрельцов А. А. Правовой подход к построению системы защиты информации в организации // Правовая информатика. 2020. № 2. С. 54–61. DOI:10.21681/1994-1404-2020-2-54-61.
2. Королев В. Т., Ловцов Д. А. Качество стандартизованной системы алгоритмов шифрования данных в ГАС РФ «Правосудие» // Правовая информатика. 2018. № 2. С. 49–59. DOI:10.21681/1994-1404-2018-2-49-59.
3. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М.: РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
4. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66–74. DOI:10.21681/1994-1404-2017-3-66-74.
5. Ловцов Д. А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. Москва: РГУП, 2020. С. 464–473. ISBN 978-5-93916-823-6.
6. Ловцов Д. А. Развитие информационной сферы общественно-производственной деятельности: достижения, угрозы безопасности и правовое регулирование // Государство и право в новой информационной реальности: Сб. науч. тр. / Отв. ред. Е. В. Алферова, Д. А. Ловцов. М.: ИНИОН РАН, 2018. С. 15–37. ISBN 978-5-248-00888-9.
7. Ловцов Д. А., Терентьева Л. В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. 2020. Т. 73. № 7. С. 115–126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
8. Ловцов Д. А., Кабелев Д. Б. Технология и проблемы рационального управления ключевой информацией в АСУ // Труды XXIX Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (24–25 июня 2010 г.) в 5-ми тт. Т. 4 / РАО. Серпухов: Серп. воен. ин-т, 2010. С. 144–148.
9. Мао В. Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.

10. Сингх С. Книга шифров: тайная история шифров и их расшифровки. М.: Аванта, 2009. 463 с.
11. Сунаид Х. А., Яковлев А. В. Состояние и перспективы развития государственной информационно-телекоммуникационной системы Йемена / Труды науч.-прак. конф. «Информационные системы и процессы» (15 июня 2018г.) / ТГУ. Тамбов: Междунар. информ. нобел. центр, 2018. С. 76–89.
12. Хучиров А. Г., Яковлев Ал. В., Яковлев Ан. В. Реализация метода кластерного анализа в математической модели процессов взаимообмена информационными ресурсами в автоматизированной системе управления специального назначения // Перспективы науки. Тамбов: «Фонд развития науки и культуры», 2017. №1. С. 75–79. ISS. 2077-6810.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. М.: Вильямс, 2016. 1024 с.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Россия.*
E-mail: vvalex1961@mail.ru

ORGANIZATIONAL AND LEGAL QUESTIONS OF IMPLEMENTING STRONG PRIVATE CRYPTOSYSTEMS

Victor Gridnev, *Ph.D., Associate, Associate Professor of the Department of Information Systems and Information Security, Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *vikadres@yandex.ru*

Ivan Volodin, *student of the Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *ivolodin98@gmail.com*

Anastasiya Zheludkova, *student of the Tambov State Technical University, Russian Federation, Tambov.*
E-mail: *anasanutasia@gmail.com*

Keywords: *legal regulation, information protection, human rights, national security, strong encryption, honest cryptosystem, encryption with escrow keys, threshold secret sharing schemes, control over the authenticity of shadows.*

Abstract.
Purpose of the work: to study the task of legal regulation of relations in the field of strong encryption of personal information of citizens in various countries and ways to solve it.
Method: system organizational and legal analysis of influence of normative and legal support on the development of private cryptographic systems.
Results: estimation of the degree of influence of regulatory documents and legislative acts on the development of cryptographic systems for private use is discussed; the most promising technology for the development of deposited encryption systems for personal information of citizens was substantiated, based on the implementation of a threshold secret sharing scheme with the ability to control the authenticity of the encryption key shadows.

References

1. Alekseev V. V., Emel`ianov E. V., Kasterin D. A., Strel`tcov A. A. Pravovoi` podhod k postroeniiu sistemy` zashchity` informatcii v organizatcii // Pravovaia informatika. 2020. № 2. S. 54-61. DOI:10.21681/1994-1404-2020-2-54-61.
2. Korolev V. T., Lovtcov D. A. Kachestvo standartizovannoi` sistemy` algoritmov shifrovaniia danny`kh v GAS RF «Pravosudie» // Pravovaia informatika. 2018. № 2. S. 49-59. DOI:10.21681/1994-1404-2018-2-49-59.
3. Lovtcov D. A. Sistemologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere : monografiia. M.: RGUP, 2016. 316 s. ISBN 978-5-93916-505-1.
4. Lovtcov D. A. Problema garantirovannogo obespecheniia informatcionnoi` bezopasnosti krupnomasshtabny`kh avtomatizirovanny`kh sistem // Pravovaia informatika. 2017. № 3. S. 66-74. DOI:10.21681/1994-1404-2017-3-66-74.
5. Lovtcov D. A. Informatcionnaia bezopasnost` avtomatizirovanny`kh blokchei`n-sistem: ugrozy` i sposoby` povy`sheniia // Tr. II Mezhdunar. nauch.-prak. konf. «Transformatciia natcional`noi` sotcial`no-e`konomicheskoi` sistemy` Rossii» (22 noiabria 2019 g.) / RGUP. Moskva: RGUP, 2020. S. 464-473. ISBN 978-5-93916-823-6.

6. Lovtcov D. A. Razvitie informatcionnoi` sfery` obshchestvenno-proizvodstvennoi` deiatel`nosti: dostizheniia, ugrozy` bezopasnosti i pravovoe regulirovanie // Gosudarstvo i pravo v novoi` informatcionnoi` real`nosti: Sb. nauch. tr. / Otv. red. E. V. Alferova, D. A. Lovtcov. M.: INION RAN, 2018. C. 15-37. ISBN 978-5-248-00888-9.
7. Lovtcov D. A., Terent`eva L. V. Pravovoe regulirovanie mezhdunarodny`kh kommercheskikh e`lektronny`kh kontraktov. Tekhnologicheskie i pravovy`e aspekty` e`lektronnoi` podpisi // Lex russica. 2020. T. 73. № 7. S. 115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126.
8. Lovtcov D. A., Kobelev D. B. Tekhnologiia i problemy` ratcional`nogo upravleniia cliuchevoi` informatciei` v ASU // Trudy` XXIKH Vseross. nauch.-tekhn. konf. «Problemy` e`ffektivnosti i bezopasnosti funktcionirovaniia slozhny`kh tekhnicheskikh i informatcionny`kh sistem» (24–25 iiunia 2010 g.) v 5-mi tt. T. 4 / RAO. Serpuhov: Serp. voen. in-t, 2010. S. 144-148.
9. Mao V. Sovremennaia kriptografiia: teoriia i praktika. M.: Vil`iams, 2005. 768 s.
10. Singkh S. Kniga shifrov: tai`naia istoriia shifrov i ikh rasshifrovki. M.: Avanta, 2009. 463 s.
11. Sunaid KH. A., Iakovlev A. V. Sostoianie i perspektivy` razvitiia gosudarstvennoi` informatcionno-telekommunikatcionnoi` sistemy` I`emena / Trudy` nauch.-prak. konf. «Informatcionny`e sistemy` i protcessy`» (15 iiunia 2018g.) / TGU. Tambov: Mezhdunar. inform. nobel. centr, 2018. S. 76-89.
12. Huchirov A. G., Iakovlev Al. V., Iakovlev An. V. Realizatciia metoda clasternogo analiza v matematicheskoi` modeli protcessov vzaimoobmena informatcionny`mi resursami v avtomatizirovannoi` sisteme upravleniia spetcial`nogo naznacheniia // Perspektivy` nauki. Tambov: «Fond razvitiia nauki i kul`tury`», 2017. №1. S. 75 — 79. ISS. 2077-6810.
13. Shnai`er B. Pricladnaia kriptografiia. Protokoly`, algoritmy` i ishodny`i` kod na C. M.: Vil`iams, 2016. 1024 s.