АНАЛИЗ ИЗМЕНЕНИЯ СУЩНОСТИ ПОНЯТИЯ «ФИНАНСОВАЯ КРИПТОГРАФИЯ» НА ОСНОВЕ 20-ЛЕТНЕЙ ТЕМАТИКИ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ «FINANCIAL CRYPTOGRAPHY AND DATA SECURITY»

УДК 330.46, 336.717

Александр Алексеевич Варфоломеев,
к. ф.-м. н., доцент кафедры Информационная безопасность Московского государственного технического университета им. Н. Э. Баумана (МГТУ)
Тел.: (495) 263 69 36
Эл. почта: a.varfolomeev@mail.ru

В статье рассматривается понятие «финансовая криптография», появившееся в 1997 году в названии одноименной конференции и использующееся за рубежом до настоящего времени наряду с такими понятиями как «квантовая криптография», «пост-квантовая криптография», «низкоресурсная (легковесная) криптография» и др. Основное внимание уделяется изменяющимся отличительным особенностям понятия «финансовая криптография», выделяющим это понятие из всей криптографии.

Ключевые слова: *информационная безопасность, криптография, финансовая криптография, электронные платежные системы, электронный бизнес, защита данных.*

Alexander A. Varfolomeev,
PhD in Math, Docent, the Department of Information Security, Bauman Moscow State Technical University (BMSTU)
Tel.: (499) 263 69 36
E-mail: a.varfolomeev@mail.ru

ANALYSIS OF THE CHANGE OF THE CONCEPT «FINANCIAL CRYPTOGRAPHY» ON THE BASIS OF 20 YEARS SUBJECTS OF THE INTERNATIONAL CONFERENCE «FINANCIAL CRYPTOGRAPHY AND DATA SECURITY»

The article discusses the concept of «financial cryptography», which appeared in 1997 in the eponymous conference title and used abroad to date along with concepts of «quantum cryptography», «post-quantum cryptography», «lightweight cryptography» and other. The focus is on changing the distinctive features of the concept of «financial cryptography» distinguishing it from the concept of the entire cryptography.

Keywords: *information security, cryptography, financial cryptography, electronic payment systems, e-business, data protection.*

1. Введение

Термин «финансовая криптография» появился в 1997 году в связи с проведением Первой Международной конференцией «Financial Cryptography» (далее – FC) и до сих пор очень широко используется за рубежом. В меньшей степени этот термин используется в России. Термин ввел по всей видимости Роберт Хеттинга (Robert Hettinga). В феврале 2016 года прошла уже 20-я конференция, но уже с несколько измененным названием «Financial Cryptography and Data Security» (далее – FC& DS). Создана Международная ассоциация по финансовой криптографии (International Financial Cryptography Association – IFCA). Все это говорит о том, что термин не случаен, он прижился и используется. Но даже беглое знакомство с тематикой прошедших конференций говорит о том, что под этот термин подводились в разное время разные направления криптографических исследований, менялась сущность или содержание понятия, обозначаемого данным термином. В связи с этим целью данной работы является рассмотрение границ данной области, ее пересечения с другими областями криптографии и информационной безопасности.

2. Предпосылки появления термина, первоначальный смысл понятия, динамика изменения тематики конференции

В первом приглашении на конференцию FC 97 ее устроители предлагали обсудить вопросы безопасности финансовых операций (transactions) в электронном (цифровом) виде. Напомним, что согласно, например, Словарю юридических и финансовых терминов, «...Финансовые операции – сделки и другие действия граждан или юридических лиц с финансовыми средствами независимо от формы и способа их осуществления…».

Конечно, основное внимание было сделано на «сделки и другие действия» в электронном (цифровом) виде.

В свою очередь, «...Финансовые средства – деньги (банкноты и металлические монеты) в валюте любой страны, государственные облигации, облигации, векселя, чеки, депозитные и сберегательные сертификаты, банковские сберегательные книжки на предъявителя, коносаменты, акции, приватизационные ценные бумаги, дебетовые и кредитовые пластиковые карточки или иные документы, удостоверяющие право на владение или передачу денежных средств, имущества, имущественных прав, реализация которого возможна только при предъявлении таких документов...».

Сразу обращает на себя внимание то, что само название конференции «Финансовая криптография» предполагает рассмотрение обеспечения безопасности финансовых операций только криптографическими методами. Можно было бы ограничиться именно этим определением. Но создатели конференции предполагали рассматривать вопросы безопасности шире. В том же приглашении на конференцию говорилось, что целью конференции было собрать вместе как специалистов в финансовой области, так и в области безопасности данных (data security) для обмена идеями. Таким образом, именуясь как «финансовая криптография», по сути конференция собиралась рассматривать «безопасность финансовых операций», что обеспечивается не только криптографическими методами.

И действительно, при подавляющем количестве технических докладов на FC 97, один из докладов был посвящен правовым вопросам в области

криптографии, которых накопилось много. Это вопросы экспорта криптографических средств, использования цифровых подписей.

Важно посмотреть на тематику первых конференций.

Большое внимание на FC 97 уделялось вопросам анонимности электронных денег. Если бумажные деньги легко обеспечивают анонимность плательщика, то в электронном мире обеспечить анонимность электронных денег могла только криптография. Интересно, что доклад, представленный на этой конференции Р. Райвестом о перспективах «финансовой криптографии», был далее им пересмотрен в аналогичном докладе на той же конференции 2006 года. В этом докладе он делает вывод, что в дальнейшем анонимность платежей будет реализовываться на практике только для микроплатежей, для очень малых сумм (доли цента, рубля, …). Анонимность платежей на большие суммы будет запрещена нормативными правовыми актами.

Возможно, чтобы сделать анонимность более приемлемой появилось понятие «отзываемой анонимности (ограниченной анонимности)», когда при определенных условиях можно восстановить личность анонима, выполнившего платеж или другие действия. Далее в перечне тем конференции значится тема «Анонимность», без указания конкретных схем или систем. Анонимность является одним из аспектов безопасности наряду с такими, как секретность, целостность, подлинность, неотказуемость (невозможность отказа от выполненных действий), которыми традиционно занималась криптография.

Многие связывают появление самой конференции с именем Д. Чаума (D.Chaum), который предложил схему подписи вслепую (Blind signature), обеспечивающую анонимность автора документа от подписывающего документ своей подписью третьего лица и используемую в схемах электронных денег и схемах электронного тайного голосования.

Появившись в середине 1990-х схемы микроплатежей в своей истории прошли как падения, связанные с успешными атаками на их безопасность, так и взлеты, связанные с появлением новых безопасных схем. Тематика микроплатежей остается до сих пор актуальной. Интенсивность исследований в этой области большая.

Следует отметить, что среди объявленных для обсуждения на конференции тем некоторые не несли специфическую связь с финансовыми операциями, а имели более широкое применение в системах безопасности. Например, такие темы как «аутентификация», «безопасность связи», «обусловленный доступ», «защита от копирования», «защита авторских прав», «электронное голосование». Наиболее явную связь с финансовыми операциями имеют темы «анонимные платежи», «кредитные / дебетовые карты», «обмен валют», «цифровая наличность (Digital Cash)», «перевод электронных денег», «электронные кошельки», «электронные бумажники», «микроплатежи», «интеллектуальные карты», «сетевые платежи», «домашний банкинг». Некоторые темы занимали промежуточное положение между финансами и криптографией. Например, «стойкость к подделке», «цифровые подписи», «цифровые квитанции». С одной стороны, не важно, какой электронный документ подписывать (то есть универсальность), с другой стороны цифровая подпись используется в электронном платежном документе. Уже на первых конференциях было заявлено о возможности рассмотрения «правовых вопросов», «вопросов регулирования», но в представленных в программе докладах их мало.

Тематика FC 98 помимо ожидаемых докладов о электронных платежных системах, содержит доклады об Интернет-коммерции (WWW-commerce) и электронной коммерции (E-commerce). Электронная коммерция, как сфера экономики, включает в себя и все финансовые, и все торговые операции (транзакции), осуществляемые при помощи компьютерных сетей, а также все бизнес-процессы, связанные с проведением таких транзакций. К электронной коммерции относят: электронный обмен информацией (Electronic Data Interchange, EDI), электронное движение капитала (Electronic Funds Transfer, EFT), электронную торговлю (e-trade), электронные деньги (e-cash), электронный маркетинг (e-marketing), электронный банкинг (e-banking), электронные страховые услуги (e-insurance). Таким образом, тематика уже выходит за рамки финансовых операций и ее впору называть «коммерческой криптографией». Далее эта тематика присутствует на всех конференциях.

Появляется тема «цифровых водяных знаков» (Digital Watermarks).

Конференция FC 99 уже организуется Международной ассоциацией по финансовой криптографии (the International Financial Cryptography Association (IFCA)). Новым является появление в докладах тем по защите интеллектуальной собственности, информационной экономике, электронным аукционам, анонимным инвестициям. Продолжается тема по цифровым подписям, именно по схемам «групповой подписи», предоставляющей подписавшему ограниченную анонимность. Отдельная секция на FC 99 посвящена стеганографии, что неожиданно.

FC 00 уже объявляется конференцией по безопасности финансовой информации и цифровой коммерции. Новой тематикой становится «безопасное подписание контракта», «электронное голосование» и «электронные лотереи». Присутствует тематика по инфраструктуре открытых ключей, которая больше присуща для конференций по криптографии.

Такие темы, как «управление рисками», «управление доверием» также можно отнести к универсальным вопросам информационной безопасности, которые конечно имеют место при финансовых операциях. Уделено внимание и техническим средствам защиты авторских прав (DRM – Digital rights management). Из криптографических тем появляется тема «многосторонних безопасных вычислений» (secure multiparty computation).

На конференции FC 03 появляется тема «экономики безопасности». Тема «Честный обмен» представлена «честным обменом цифровыми подписями».

2005 год стал знаковым для конференции – она поменяла название на «Финансовая криптография и безопасность данных» (Financial Cryptography and Data Security), чтобы охватить все вопросы безопасности транзакций и систем. Фактически название стало больше отражать тематику конференции, но не полностью. Видимо было желание сохранить узнаваемость конференции, не изменяя полностью название.

На FC&DS 09 появляется тема «обнаружения мошенничества» (Fraud Detection). Слово «фрод» стало часто употребляться и в русском языке, а борьба с фродом присутствовать при проведении финансовых (банковских) операций. Большое место на FC 2009 было уделено так же «Экономике информационной безопасности».

Новым для конференции FC&DS 10 стали вопросы безопасности электронных паспортов (e-Passports) и низкоресурсной (легковесной) криптографии (Lightweight Cryptography), имеющие самостоятельное значение и применение.

Среди тем FC & DS 11 надо выделить протоколы «безопасного ознакомления с информацией» (Private Information Retrieval), позволяющие эффективно скачивать разделы баз данных с финансовой информацией без раскрытия для держателей этих баз, что скачивается.

На применение криптографических схем и протоколов в финансовой области существенное влияние оказывает развитие методов атак, не все из которых представлены на данной тематической конференции. Например, на FC & DS 11 рассматривается атака на протокол SSL, но атака «POODLE», разработанная в 2014 году и положившая конец широкому использованию известных протоколов SSL и протокола TLS версии ниже 1.1, не представлена на конференции.

В 2012 году с опозданием впервые на конференции стала присутствовать тематика широко известной в настоящее время криптовалюты Биткоин (bitcoin), использующей технологию Блокчейна (криптографические хэш функции). Наблюдается запаздывание в рассмотрении проблем криптовалюты Биткоин и на криптографических конференциях. Первая работа с описанием Биткоин за авторством Сатоши Накамото появилась в 2008 году. Еще раньше, как считается, представили свои работы по близкой тематике Дэвид Чаум, Стефан Брандс, Адам Бэк, Вей Даи, Ник Забо, Хал Финней. Но именно в это время эта криптовалюта стала заметным явлением. Далее тема Биткоин присутствует на всех последующих конференциях FC&DS.

На конференции FC&DS 2016 с докладом «Финансовая криптография: прошлое, настоящее и будущее» выступил Ади Шамир и сформулировал 15 предложений – прогнозов. Большинство из них более связано с проблемами криптографии и информационной безопасности в целом. Например, что алгоритмы AES и SHA-2/3 останутся безопасными (в отличии от RC4 и SHA-1), размер ключей превысит 2048 бит до 4096, технология «Интернет вещей» будет не безопасной, кибервойны будут нормой при конфликтах, квантовые компьютеры для атак на RSA ключи созданы не будут, хотя правительства будут тратить большие деньги на исследования. Ближе всего к финансовой криптографии прогноз, что Биткоин исчезнет, но оставит наследие, а технология Блокчейн будет превозноситься, но успешно применяться в ограниченных условиях. Повторяет Шамир и давний прогноз Райвеста о том, что правительства не потерпят анонимности. Наконец, Шамир предрекает бесконечный поток новых платежных механизмов, что звучит оптимистично для исследователей и практиков финансовой криптографии.

3. Финансовая криптография в российских условиях

Наиболее близкой по тематике к международной конференции «Финансовая криптография и безопасность данных» является конференция РусКрипто, проводимая в нашей стране с 1999 года. На ней присутствует как криптографическая секция, так и секции, рассматривающие вопросы применения криптографии, вопросы информационной безопасности новых технологий, правовые и организационные вопросы, вопросы разработки и внедрения новых международных и отечественных стандартов и рекомендаций.

Близкими по тематике являются также следующие конференции:

Конференция «Информационная безопасность платежных систем. PCI DSS Russia»;

Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи. «PRI-Форум Россия»;

Форум Ассоциации Защиты Информации «Актуальные вопросы информационной безопасности»;

Уральский форум «Информационная безопасность банков», проводимый при официальной поддержке Банка России.

В настоящее время в России регулируется и криптография и информационная безопасность, а также банковское дело, включая перевод денежных средств. Уже принятые нормативные документы накладывают свои ограничения на применение мер безопасности в этих областях. Не имея возможности перечислить все нормативные акты, можно упомянуть в качестве примеров Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», Положение Банка России от 9 июня 2012 г. № 382-П, Постановление Правительства РФ от 16 апреля 2012 г. № 313. Развивается система стандартов и лучших практик. Здесь особо надо упомянуть Банк России, создавший стандарт СТО БР ИББС-1.0. По-прежнему действует обязательный стандарт по пластиковым картам PCI DSS 3.2, обновивший свою версию в апреле 2016 года. Но все же можно сказать, что в основном финансовая криптография у нас в стране представлена банковской сферой деятельности.

В настоящее время идет дискуссия о создании российской криптовалюты. Отечественная криптография может предоставить необходимые средства. Но если использование технологии Блокчейна не вызывает сомнения, то по поводу анонимности и контролируемости эмиссии криптовалюты в прессе высказываются различные мнения. Пока трудно сказать, какой будет

российская криптовалюта, но она по-видимому будет и надо готовиться к ее появлению.

4. Заключение

Конференция, давшая название термину «Финансовая криптография», давно расширила тематику своих докладов, и, хотя изменила свое название на «Финансовая криптография и безопасность данных», по сути рассматривает вопросы безопасности электронной коммерции, включающей финансовые операции.

Но понятие и термин «финансовая криптография» имеет под собой конкретную основу, которую можно определить как обеспечение информационной безопасности финансовых операций в электронном (цифровом) виде криптографическими методами, включая разработку и анализ криптографических схем и протоколов в области электронных платежей (микроплатежей), электронных денег, криптовалют, применения интеллектуальных карт, цифровых водяных знаков, электронных аукционов, специальных схем цифровой(электронной) подписи, с учетом отечественных и международных стандартов и рекомендаций.

Область применения «финансовой криптографии» существенно изменилась с момента возникновения этого понятия. Если ранее криптография обеспечивала безопасность операций с финансовыми средствами, представленными в электронной форме, то в настоящее время, помимо этого, криптография сама предоставляет финансовые средства в виде криптовалют, не имеющие физической основы в реальном мире.

Без применения криптографии решить вопросы безопасности в финансовой сфере просто невозможно. Но криптографические методы, как и все другие технические методы защиты информации, должны на практике рассматриваться и применяться вместе с организационными и правовыми методами. Но это предмет отдельного рассмотрения.

В дальнейшем понятие «финансовая криптография» следует различать с понятиями «коммерческая криптография», «промышленная криптография», «бизнес криптография» и другими, которые могут включать разделы «финансовой криптографии».

Литература

1. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М: МИФИ, 1997. 274 с.

2. Отставнов М. Финансовая криптография для «чайников» // Конфидент. – 1999. – № 6.

3. Варфоломеев А.А., Запечников С.В., Маркелов В.В., Пеленицын М.Б. Интеллектуальные карты и криптографические особенности их применений в банковском деле: учебное пособие. – М.: МИФИ, 2000. – 188 с.

4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 07.06.2016).

5. Rosenberg B. Handbook of Financial Cryptography & Data Security. – CRC Press, 2011. – 612 p.

6. Сычев А.М., Ревенков П.В., Дудка А.Б. Безопасность электронного банкинга. – М.: РФК – Имидж Лаб, 2016. – 188 с.

References

1. Anohin M.I., Varnovskij N.P., Sidel'nikov V.M., Jashhenko V.V. Kriptografija v bankovskom dele. – M: MIFI, 1997. 274 s.

2. Otstavnov M. Finansovaja kriptografija dlja «chajnikov» // Konfident. – 1999. – № 6.

3. Varfolomeev A.A., Zapechnikov S.V., Markelov V.V., Pelenicyn M.B. Intellektual'nye karty i kriptograficheskie osobennosti ih primenenij v bankovskom dele: uchebnoe posobie. – M.: MIFI, 2000. – 188 s.

4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 07.06.2016).

5. Rosenberg B. Handbook of Financial Cryptography & Data Security. – CRC Press, 2011. – 612 p.

6. Sychev A.M., Revenkov P.V., Dudka A.B. Bezopasnost' jelektronnogo bankinga. – M.: RFK – Imidzh Lab, 2016. – 188 s.