Кудрявцев Олег Анатольевич. Страхование в системе управления рисками инфраструктуры открытых ключей : Дис. ... канд. экон. наук : 08.00.10 : Москва, 2003 129 c. РГБ ОД, 61:03-8/3605-6

**Содержание к диссертации**

Введение

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ РИСКАМИ 12

1.1. Сущность и классификации рисков 12

1.2. Риск-менеджмент как управленческий процесс 23

ГЛАВА II. ОСНОВНЫЕ ЭЛЕМЕНТЫ И ПРИНЦИПЫ ПОСТРОЕНИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ 35

2.1. Инфраструктура открытых ключей: понятие, составные элементы, принципы функционирования 35

2.2. Организационный аспект механизма функционирования удостоверяющего центра 45

ГЛАВА III. УПРАВЛЕНИЕ РИСКАМИ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ 51

3.1. Распределение рисков участников инфраструктуры открытых ключей 51

3.2. Отдельные риски, связанные с особенностями построения инфраструктуры открытых ключей и ее правового регулирования в России 58

3.3. Управление рисками удостоверяющего центра 72

3.3.1. Виды рисков удостоверяющего центра, средства и методы управления ими...72

3.3.2. Обоснование возможной схемы страховой защиты удостоверяющего центра .90

3.4. Основные условия новых видов страхования рисков субъектов

инфраструктуры открытых ключей 98

3.4.1. Страхование профессиональной ответственности удостоверяющего центра 98

3.4.2. Страхование владельцев сертификатов 108

ЗАКЛЮЧЕНИЕ 121

СПИСОК ЛИТЕРАТУРЫ 124

**Введение к работе**

Актуальность исследования. Двадцать первый век по праву можно считать веком информационных технологий. Они уже стали частью нашей повседневной жизни, однако сферы их применения в социальной и экономической жизни общества продолжают расширяться темпами, во много раз превосходящими темпы развития всех других технологий, которые до этого придумало человечество. За 10 лет своего существования Интернет смог объединить мир в единую информационную инфраструктуру, которая дает человеку неограниченные возможности в плане бизнеса, образования, обмена информацией и опытом. Без преувеличения можно говорить о том, что информационные технологии за последние несколько лет определили основные направления развития общества в целом и человека в частности.

Влияние информационных технологий на экономические процессы также очень велико. Пока еще предстоит подвести итоги экономического бума конца 90-х, связанного с всплеском интереса к Интернет-бизнесу, а также последовавшего за ним спада. Еще пока нет методик, которые позволили бы исследователям дать количественную оценку связи темпов экономического роста и роста продуктивности с внедрением в корпоративную среду информационных технологий. Однако даже те цифры, которые есть, свидетельствуют о том, что тенденция дальнейшего позитивного развития информационных и Интернет-технологий сохранится. Только за предыдущий год, ставший не самым лучшим годом Интернет-бизнеса, обороты электронной коммерции выросли более чем на 70%, с 354 до 615 миллиардов доллларов, а число пользователей Интернет достигло 497,7 миллионов человек по всему миру.1

Одновременно с неоспоримыми преимуществами, которые дают компьютерные технологии в области информационного обмена и электронной коммерции, они несут с собой и много подводных камней. Пожалуй, основной среди них - вопрос безопасности. Это многогранная проблема, которая имеет множество проявлений, а потому так или иначе затрагивает всех участников информационного обмена. К примеру, для простого пользователя Интернет проблема безопасности связана с возможностью несанкционированного доступа к данным, хранящимся на его компьютере, или заражение компьютерным вирусом; для покупателя Интернет- 1 Western Europe Pulls Ahead of United States, IDC Newsletter, 03 января 2002,

Страница 3 магазина - опасность хищения сведений о его кредитной карточке; для предприятия, заключающего контракт в электронном виде - отсутствие уверенности в том, что контрагент, с которым он не знаком лично и который находится на другом конце света, окажется действительно надежной компанией, а не мошенником. До сих пор проблема безопасности остается краеугольным камнем развития Интернет, существенно сдерживающим прогресс в областях, требующих обеспечения надежного и конфиденциального обмена информацией, а более всего - в электронной коммерции. Так, в ходе опроса, проведенного компанией Jupiter, 58% респондентов заявили, что отказывались от покупки, заходя на тот или иной Интернет-сайт, по соображениям безопасности1.

Универсального средства, позволяющего снять если не все, то большинство проблем с безопасностью, до сих пор, наверное, не существует. Однако за последние несколько лет решения, претендующие на универсальность, все-таки начали появляться. Среди них особо следует отметить системы, основанные на асимметричной криптографии или криптографии с открытыми ключами. Сейчас уже можно утверждать, что эти технологии положены в основу инфраструктуры информационной безопасности во многих странах мира, в том числе и в России. Предполагается, что многоуровневая инфраструктура открытых ключей (ИОК), которая будет создана на национальном уровне, позволит решить многие проблемы электронной коммерции и расширит сферы использования электронного обмена данными. Вместе с тем, как показывает опыт, любая новая технология связана с возникновением новых рисков, которые на первый взгляд неочевидны, однако в перспективе могут приводить к значительным убыткам для всех участников экономической деятельности. Важность роли ИОК, одной из целей которой является обеспечение гарантий интересов всех сторон, вовлеченных в электронную коммерцию, диктует необходимость тщательного анализа потенциальных рисков, которые связаны с применением данной технологии. Не случаен огромный интерес к этой проблеме со стороны представителей бизнеса и органов государственной власти, в чьи обязанности вменяется разработка необходимой законодательной и нормативной базы.

Ключевую роль в обеспечении надежной работы ИОК может играть страхование. Федеральный Закон "Об электронной цифровой подписи" предусматривает, что "... удостоверяющий центр должен обладать необходимыми 1 Overhyped and Misunderstood: The Fraud of Online Fraud, Jupiter Research, 2002.

Страница 4 материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей"1. Одним из основных финансово-экономических механизмов обеспечения таких гарантий является страхование, требования в отношении которого станут, как предполагается, частью нормативной базы, регулирующей деятельность удостоверяющих центров.

Несмотря на чрезвычайную актуальность темы, необходимо отметить ее недостаточную проработанность в научной литературе: какие-либо специальные исследования по ней отсутствуют, причем как в России, так и за рубежом. Проблема анализа рисков ИОК носит комплексный характер, поскольку находится на стыке технических, юридических и экономических наук. Однако рассмотрение вопросов создания и функционирования ИОК в литературе шло раздельно по этим составляющим, что не позволило сформировать целостный и системный подход к проблеме. Так, достаточно подробно в зарубежной литературе рассматриваются юридические последствия введения и применения национальных законодательных актов об электронных цифровых подписях2. Хорошо проработана теоретическая база криптографии с открытыми ключами и ее применение в построении комплексных систем безопасности электронной коммерции3, описаны технические и технологические особенности, проанализированы плюсы и минусы различных систем4

Весьма полезными в понимании принципов функционирования инфраструктуры открытых ключей представляются работы, описывающие опыт США 1 ФЗ №1 от 10.01.02 "Об электронной цифровой подписи", ст. 8. 2 См. Bill Zoelick. Commentary on the Electronic Signatures in Global and National Commerce Act, 2001. . Bradford Biddle. Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key

Infrastructure, San Diego Law Review, n.33, October 1996. Lawrence Lambert. The New Electronic Signatures in Global and National Commerce Act: How effective is it?, 3 См. R.L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol.21, Nr.2, 1978. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 1996,

Marc Branchaud. A Survey of Public Key Infrastructures, March 1997, 4 См., напр. Michael S. Baum. Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of "Equivalence", VeriSign, 1999. Roger Clarke. Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society, 13/11/00,

Страница 5 в построении американской федеральной инфраструктуры1. Тем не менее, экономическая часть проблемы, связанная с оценкой эффективности функционирования механизмов ИОК, а также возникающих в связи с этим потерь, практически не нашла отражения в открытой литературе. Недостаточна ее проработанность и в практическом плане: у руководителей создаваемых сейчас в России удостоверяющих центров зачастую отсутствует представление о потенциальных угрозах, связанных с функционированием инфраструктуры открытых ключей, методах их оценки и минимизации. За исключением нескольких работ2, так или иначе затрагивающих вопросы рисков, подавляющее большинство материалов носит недостаточно проработанный и узкий характер3.

Как видно, все перечисленные материалы написаны зарубежными авторами. Это не случайно. В России обсуждение данных вопросов проходило с отставанием в 2-3 года от ведущих западных стран и, в первую очередь, от США. Поэтому, в частности, степень охвата и глубина проработанности проблем создания инфраструктуры открытых ключей в нашей литературе на порядок ниже.

В России обсуждение проблем создания отечественных механизмов инфраструктуры открытых ключей в основном началось в период разработки федерального законодательства об электронной цифровой подписи и электронной коммерции. Среди наиболее значимых мероприятий, где рассматривались данные проблемы, можно назвать 1-ю и 2-ю Всероссийские конференции "Информационная безопасность в условиях глобального информационного общества" (Москва, 9 февраля 2001 года и 18 июня 2001 года), Всероссийскую конференцию "Безопасность телекоммуникационных и информационных технологий для взаимодействия граждан, бизнеса и органов государственной власти" (Москва, 27-29 марта 2002 года), Международный Интернет-форум "Состояние и перспективы развития Интернета в России" (Москва, 12-14 сентября 2001 года) и др.

Несколько слов о другом аспекте проблемы - точке зрения страховщиков на управление рисками, связанными с информационными технологиями. Здесь 1 См. Kathy Lyons-Burke. Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, National Institute of Standards and Technology, Special Publication 800-25, October 2000. Richard Kuhn et al. Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institute of Standards and Technology, 26 February 2001, 2 Cm. Carl Ellison, Bruce Schneier. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal, n. 1, 2000, pp. 1-7, Carl Ellison and Bruce Schneier. Risks of PKI: Electronic Commerce, Inside Risks 116, Communications of the ACM, vol 43, n2, Feb 2000, Michael S. Baum. Federal Certification Authority Liability and Policy. US Department of Commerce, N1ST, 1999. 3 См., напр. Public Key Infrastructure: The Risks for Financial Institutions Involved with PKI, Ernst&Young, 2001.

Страница 6 ситуация следующая: в то время как теоретические вопросы, касающиеся, прежде всего, общих направлений страхования, и, в несколько меньшей степени, управления рисками, проработаны очень полно - достаточно перечислить известные работы отечественных1 и зарубежных2 авторов, часть проблемы, связанная со страхованием специфических компьютерных рисков, вообще никак не отражена в литературе. Вызвано это тем, что страхование рисков, связанных с информационными технологиями, или, другими словами информационных рисков, является новым и перспективным направлением для отечественных и зарубежных страховщиков. На Западе его история не насчитывает и 5-ти лет, а активная выдача подобных полисов началась лишь в 2000-м году. В изучении данного вопроса сейчас можно ориентироваться лишь на практический опыт и доступные методические материалы страховых компаний, таких как AIG, АХА, Chubb, Hiscox - за рубежом и Ингосстраха - в России. Хотя информация о страховых продуктах в этой области до сих пор рассматривается страховщиками как ноу-хау и коммерческая тайна\* а потому не выходит за пределы офисов компаний. В процессе реализации проекта по страхованию информационных рисков Ингосстрахом была собрана определенная база таких материалов, часть из которых была крайне полезна при написании данной работы.

Целью настоящей работы является теоретическое обоснование и практическое решение проблемы использования страхования в системе управления рисками инфраструктуры открытых ключей. Для достижения данной цели предполагается решить следующие задачи:

Провести анализ теоретических основ управления рисками

Обобщить организационные особенности функционирования инфраструктуры открытых ключей

Проанализировать риски инфраструктуры открытых ключей, определить механизмы управления ими, в том числе обосновать основные положения новых видов страхования в этой области.

Помимо указанных цели и задач, в диссертации имеется еще ряд частных моментов, которые вытекают из существа рассматриваемых вопросов и оказывают 1 См., напр. Балабанов И.Т. Риск-менеджмент - М., 1996, Гомелля В.Б. Основы страхового дела - М., 1998, Уткин Э.А. Риск-менедежмент - М., 1998, Хохлов Н.В. Управление риском - М, 1999, Шахов В.В. Страхование. - М., 1997, Шахов В.В. Введение в страхование - М., 1999 и др. 2 Бланд Д. Страхование: принципы и практика - М, 1998, Mark S. Dorfman. Introduction to Risk Management and Insurance, 7th Edition, Prentice Hall, 2001, George Rejda. Principles of Risk Management and Insurance, 8th Edition, Addison-Wesley Publishing, 2002 и др.

Страница 7 влияние на структуру и стиль изложения материала. Так, в работе предполагается:

Рассмотреть риски, специфичные для ИОК, т.е. риски, определяемые особенностями применяемых при ее построении бизнес-моделей и технологий в широком смысле этого слова. Отсюда риски, носящие общий характер для всех субъектов хозяйствования, не будут предметом исследования. По этой же причине в отношении удостоверяющих центров будут проанализированы только операционные риски, а кредитные, политические и другие риски останутся за рамками рассмотрения.

Провести анализ, который носил бы достаточно общий характер и не зависел от специфики конкретного удостоверяющего центра и особенностей тех или иных технологических решений, но в то же время был бы полезен с точки зрения применения на практике на уровне компании. В этом плане предполагается детально, на микроэкономическом уровне, рассмотреть риски центрального звена ИОК - удостоверяющих центров/центров регистрации.

В отношении других участников ИОК анализ рисков будет носить общий, схематичный характер, поскольку в рамках одной работы невозможно учесть и разобрать внутреннюю специфику столь широкого круга лиц, участвующих в процессе электронной коммерции - ими могут быть электронные магазины, банки, профессиональные участники фондового рынка, производственные предприятия и предприятия сферы услуг, граждане, государственные институты.

В дополнение к этому будет дан анализ ряда факторов, которые оказывают существенное влияние на уровень рисков всех или отдельных групп участников ИОК либо сами по себе являются источником риска. Эти факторы связаны с самими технологиями, лежащими в основе ИОК, а также особенностями ее правового регулирования в России на сегодняшний день. Как будет показано далее, создаваемой в России ИОК изначально присущи определенные недостатки, которые существенно повышают вероятность возникновения потерь в процессе ее функционирования. Некоторые из этих недостатков могут быть сняты на микроуровне, т.е. самими участниками ИОК, некоторые - нет. Но и те, и другие следует учитывать при планировании и ведении бизнеса.

3. Дать практические рекомендации по альтернативному снижению и перераспределению рисков. Не случайно в названии работы есть словосочетание "управление рисками". Сегодня уже сотрудничество страховой компании и ее клиента не ограничивается выдачей полиса и последующей оплатой убытка.

Страница 8

Процесс взаимодействия носит более сложный характер: страховая компания должна совместно с клиентом попытаться проанализировать риски последнего и дать рекомендации в отношении мероприятий, которые требуются для повышения рискозащищенности страхуемых объектов и надежности бизнеса клиента. Очевидно, что любая страховая компания заинтересована в том, чтобы сформировать портфель качественных и прогнозируемых рисков. Но политика чистой селекции рисков, при которой объекты, связанные с повышенным риском, отсекаются, уже оказывается неэффективной. На смену ей приходит политика "управления рисками".

4. На основе анализа рисков дать рекомендации по построению страховой защиты удостоверяющих центров и в рамках этого сформулировать основные положения недостающих звеньев страховой защиты удостоверяющих центров. Страховые продукты, имеющиеся на момент написания работы на отечественном рынке, не покрывают всех потребностей страхования рисков в сфере информационных технологий. В этом плане потребуется разработка новых видов страхования, а также адаптация ряда существующих. Не лучше обстоит ситуация и за рубежом, где специализированные продукты, ориентированные на ИОК, также отсутствуют. Поэтому за исключением двух-трех полисов страхования ответственности удостоверяющих центров, которые еще пока слабо проработаны и практически не отличаются от типовых полисов страхования ответственности Интернет-компаний, опираться на зарубежный опыт не представляется возможным.

Объектом исследования является современный страховой рынок.

Предметом исследования являются вопросы управления рисками инфраструктуры открытых ключей, прежде всего посредством их страхования.

Теоретической основой диссертации явились труды отечественных и зарубежных авторов по теории риска, страхованию и управлению рисками, а также проблемам, касающимся функционирования систем безопасности, построенных на технологиях криптографии с открытыми ключами, исследованные в настоящей работе.

Методологической основой диссертации является система общенаучных методов - логического и системного анализа и синтеза, в т.ч. экономического сравнения и обобщения, применяемых при работе с теоретическими источниками, научно-практическими и методологическими материалами, а также при исследовании практического опыта Ингосстраха и зарубежных страховых компаний.

Страница 9

Научная новизна работы состоит в следующих положениях:

В работе проведен теоретический анализ содержания и особенностей операционных рисков, уточнено их соотношение с другими видами рисков (стр. 12-23).

Впервые проведено комплексное исследование рисков различных участников (субъектов) инфраструктуры открытых ключей, проанализированы сценарии рисков владельцев цифровых сертификатов и лиц, полагающихся на сертификаты (стр.51-58).

Проанализированы риски удостоверяющих центров электронной цифровой подписи. При этом выявлены основания возникновения гражданской ответственности удостоверяющего центра, а также предложены механизмы управления рисками удостоверяющего центра (стр. 75-89).

На основе проведенного исследования теоретических и практических основ управления рисками инфраструктуры открытых ключей дано обоснование системы страховой защиты удостоверяющего центра (стр. 90-97).

Сформулированы основные и существенные условия страхования гражданской (профессиональной) ответственности удостоверяющего центра электронной цифровой подписи, а также условия страхования владельцев цифровых сертификатов (стр.91, 98-120). В ходе анализа условий страхования предложена классификация исключений из страхового покрытия (стр. 104-105).

Настоящее исследование направлено на теоретическое обоснование и практическое решение проблемы управления рисками, связанными с функционированием инфраструктуры открытых ключей в России.

Практическая значимость и апробация работы состоит во внедрении ее положений при организации систем управления рисками в рамках создаваемой в России инфраструктуры открытых ключей, а также при осуществлении страхования специфических информационных рисков в данной области. Результаты настоящего исследования были озвучены автором на многочисленных конференциях и научно-практических семинарах, в том числе Международной конференции "Состояние и перспективы развития Интернета в России" (Москва, 13-15 сентября 2000 года), доклад "Риски электронного бизнеса: анализ проблемы и возможные сценарии"; Всероссийской конференции "Безопасность телекоммуникационных и информационных технологий для взаимодействия граждан, бизнеса и органов

Страница 10 государственной власти" (Москва, 27-29 марта 2002 года), доклад "Новые направления страхования инфокоммуникации", Научно-практических семинарах Научно-технического центра Ассоциации российских банков (Института банковского дела АРБ) и других конференциях и семинарах. Результаты исследования использованы в практической деятельности ОСАО "Ингосстрах" в ходе реализации проекта "Страхование информационных рисков", в том числе при проведении работ по анализу рисков и заключении договоров страхования. Часть из положений настоящей работы положена в основу "Правил страхования информационных систем", разработанных автором, на которые ОСАО "Ингосстрах" получило лицензию в апреле 2002 года. Правила по двум другим специальным видам страхования также предполагается провести через процедуру лицензирования и использовать в практической деятельности компании.

Основные положения и результаты исследования отражены также в 11 публикациях общим объемом 4 п.л.

Структура диссертации определяется целью и задачами, которые поставлены в работе. Диссертация состоит из введения, трех глав, заключения и списка использованной литературы.

Страница 11

## Сущность и классификации рисков

Как следует из названия настоящего раздела, в нем анализируются две проблемы - сущность и классификации рисков. Риск - понятие, которое употребляется в повседневной жизни и притом зачастую в разных смыслах. Проследить различия в определениях риска по разным источникам уже само по себе довольно интересная задача. Если проанализировать ситуации, когда нам приходится использовать понятие "риск", все их можно свести к трем группам: в первом случае риск рассматривается как некое предполагаемое событие (биржевой кризис или ураган, например), во втором: риск - вероятностная оценка наступления этого события, в третьем - это стоимостная/качественная оценка возможных потерь. Думается, что с точки зрения экономической науки, наиболее актуальна стоимостная оценка возможных потерь, наименее - характер события, с которым ассоциируется риск. Хотя для анализа, понимания и оценки рисков одинаково важны все три составляющие, которые являются неотъемлемыми характеристиками риска как целостного понятия.

Определения понятия "риск" строятся вокруг указанных трех смыслов, но, как правило, отражают только один или два из них. Какие? Это диктуется теми практическими задачами, под которые приводится определение, и ниже дается более детальный анализ этих определений.

Так, можно встретить такое определение: риск - предполагаемое событие, обладающее признаками вероятности и случайности, наступление которого связано с возможностью потерь. Данное определение содержится в подавляющем большинстве правил страхования и обобщает положения ст. 9 Закона РФ №4015-1 от 27.12.92 "Об организации страхового дела в Российской Федерации" (ред. 25.04.02) и ст. 929 Гражданского кодекса РФ, часть II. Очевидно, что здесь "риск" раскрывается через "предполагаемое событие".

С другой стороны, уже ставшая общепринятой в зарубежном финансовом сообществе методика оценки рисков "value at risk - VaR" имеет дело с рисками как с вероятностно-стоимостной категорией. Риск в данном случае выражается как "степень неопределенности будущих чистых доходов"1. Возможно, это связано с тем, что изначально задается классификация событий, которые могут привести к потерям, и потом для анализа уже не столь важно, какое из них наступит, а гораздо важнее насколько будущие доходы будут отличаться от прогнозируемых. Опять же, здесь стоит конкретная цель - оценить возможный уровень потерь в стоимостной форме.

Есть и другие определения, менее четко отражающие то, в каком из смыслов определяется понятие "риск". К примеру, И.Т. Балабанов дает такое определение: "Риск - возможная опасность потерь"1. Очевидно, что данное определение недостаточно конкретно для того, чтобы быть принятым за основу, поскольку не ясно, в каком значении употребляется термин "опасность". Кроме того, слово "возможная", которое, по нашему мнению, не несет в данном определении смысловой нагрузки, следовало бы заменить на слово "предполагаемая". Необходимо отметить, что даже самые известные отечественные авторы не всегда однозначны в том, что касается понятийного аппарата. Так, В. Шахов считает, что "...опасность неблагоприятного исхода на одно ожидаемое явление, называется риском"2. В данном случае внимание читателя акцентируется на вероятностной природе риска. Однако там же, на странице 35 приводится совершенно другое определение риска: "риск - это конкретное явление или совокупность явлений (событий или совокупность событий), при наступлении которых производятся выплаты из ранее образованного централизованного страхового фонда в натурально-вещественной или денежной форме". В другой работе В. Шахова "Страхование" определения риска нет вообще, речь идет лишь о "страховом риске", в отношении которого дается целых 4 различных определения3. Еще более подчеркивая комплексный характер понятия "риск" и вытекающую из этого возможность его плюралистической трактовки, Д. Бланд приводит 5 различных определений риска4

## Инфраструктура открытых ключей: понятие, составные элементы, принципы функционирования

Следует сразу оговориться, что цель настоящей главы - ознакомить заинтересованного читателя с назначением и общими принципами работы инфраструктуры открытых ключей. Больший акцент предполагается сделать на организационно-экономических, нежели на технических вопросах. В рамках поставленных целей и задач работы, а также учитывая ее экономическую направленность, проводить детальный и глубокий научный анализ технических аспектов решения проблемы представляется нецелесообразным.

Большинство самых распространенных современных решений по защите информации построено на базе криптографии, которая лежит и в основе рассматриваемой в данной работе инфраструктуры открытых ключей. Криптографическое преобразование (шифрование) - взаимно-однозначное математическое преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации (представленной в некоторой цифровой кодировке) блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.1 В целом это определение по своему содержанию и логике соответствует определению, официально закрепленному в нормативных документах2.

Если рассматривать информационный обмен применительно к электронной коммерции, то его эффективное осуществление невозможно без решения следующих задач1:

1. Защиты информации (Конфиденциальность). Доступ к информации должен быть ограничен лицами, которые имеют на это соответствующие права.

2. Целостности - получатель сообщения должен иметь гарантии тому, что информация, содержащаяся в сообщении, не была несанкционированно изменена в процессе его хранения и пересылки.

3. Аутентификации - возможности однозначно определить отправителя сообщения.

4. Неотрекаемости (non-repudiation) - отправитель сообщения не должен иметь возможности отказаться от сообщения под предлогом, что оно отправлено не им.

Оставив за рамками работы анализ различных систем построения информационной безопасности, отметим лишь, что в полное мере эти задачи позволяет решить асимметричная криптография или криптография открытых ключей. Это сравнительно новая технология. Ее теоретические основы были заложены в 1976 году Диффе и Хеллманом (Diffe и Hellman), а уже в 1977 году была разработана первая система, основанная на технологии открытых ключей - RSA Cryptosystem.2. В настоящее время существует множество различных реализаций технологии асимметричной криптографии, но все они объединены единым принципом работы. Он заключается в следующем: существует два ключа - один секретный, известный только отправителю сообщения, а второй - открытый, который может быть доступен любому желающему. Эти два ключа связаны между собой специальным образом: они как бы дополняют друг друга на основе математической функции. Так, зная открытый ключ, невозможно3 вычислить секретный ключ и наоборот. Вместе с тем, сообщение, зашифрованное секретным ключом, можно расшифровать только открытым ключом. Соответственно, расшифровав сообщение открытым ключом, получатель может быть уверенным в том, что это сообщение зашифровано человеком, который владеет секретным ключом. Если известно, кому принадлежит открытый, а следовательно, и секретный ключ, известен и автор сообщения. Таким образом, автор сообщения, шифруя его своим секретным ключом4, ставит своего рода подпись, т.е. преобразует сообщение так, как никто другой этого сделать не может. В этом состоит суть принципа электронной цифровой подписи (далее - ЭЦП).

Поскольку открытый ключ используется лишь для подтверждения принадлежности документа автору, держать его в тайне бессмысленно и он публикуется в открытом доступе. Здесь мы говорим, что основная задача криптографии открытых ключей в том приложении, в каком мы ее сейчас рассматриваем, смещается в сторону подтверждения авторства (аутентификации) и целостности электронного сообщения. Это принципиально важно для эффективного осуществления электронной коммерции. Защита информации, т.е. фактически то, для чего и используется шифрование в обычном понимании, уходит на второй план. Хотя функции по защите информации также реализуются с помощью криптографии открытых ключей.

Фактически, применяя открытый ключ для расшифровки сообщения, адресат получает подтверждение двух фактов:

- сообщение действительно принадлежит лицу, в чьем распоряжении был секретный ключ;

- сообщение не было незаконно модифицировано в процессе пересылки.

Однако наличие электронной цифровой подписи документа само по себе еще не решает всех проблем. Предположим, что пользователь А хочет проверить, действительно ли полученное им сообщение отправлено пользователем Б. Для того чтобы это сделать, он должен сначала каким-то образом получить открытый ключ пользователя Б. Он может получить его из рук пользователя Б при личной встрече. Однако сделать это в условиях Интернет, когда пользователи подчас расположены на разных континентах, не всегда возможно; другого надежного канала, как правило, у пользователей Интернет нет.

## Распределение рисков участников инфраструктуры открытых ключей

Проблема анализа рисков ИОК стала актуальной еще до массового распространения новой технологии в корпоративной среде и на национальном уровне стран, разрабатывавших и принимавших соответствующее законодательство. Необходимо было провести тщательную оценку технологических и бизнес-решений, применяемых в ИОК, с точки зрения снижения потенциальных потерь для всех сторон, которые могут быть затронуты в процессе ее деятельности. Думается, что на уровне компаний, уже тогда имевших корпоративные удостоверяющие центры, определенная работа в этом направлении была сделана.

Однако в открытой прессе и в Интернет вопрос анализа рисков ИОК сразу же превратился в инструмент политической борьбы, направленный на продвижение разработчиками своих технологий. Развернулась дискуссия между сторонниками биометрии и криптографии, иерархических и неструктурированных систем ИОК и т.д.1. В ситуации, когда шло обсуждение преимуществ и недостатков различных систем с целью выбора оптимального решения и закрепления его в качестве модели в новом законодательстве, это было вполне закономерно. И хотя в целом такая ситуация не могла пойти на пользу делу, поскольку картина с анализом рисков получалась несколько фрагментарной, определенный опыт по этой проблеме был все же накоплен. Появились публикации, которые рассматривали отдельные виды рисков, такие как, например, риски, связанные с ответственностью удостоверяющих центров2, или риски применительно к отдельным отраслям экономики3. Попытки же сформировать целостную картину системы рисков, связанных с внедрением ИОК, получались довольно бессистемными. Примером могут служить выпущенные американским правительством разъяснения по вопросам построения федеральной системы ИОК, которые содержат раздел, посвященный анализу рисков.1 Тем не менее, многие аргументы, высказывавшиеся западными аналитиками, были действительно справедливыми, и часть их отражена в настоящей работе.