Математическое моделирование

Математические модели оценки сохранности при передаче цифровых данных в цифровой экономике*

А.В. Соловьев[I], А.Ю. Даниленко[I], Г.П. Акимова[I], Д.С. Богданов[I], М.А. Пашкин[I], Е.В. Пашкина[I], А.А. Подрабинович[I], И.В. Туманова[I]

[I] Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва, Россия

Аннотация. В данной статье описаны математические модели оценки сохранности цифровых данных при их передаче между хозяйствующими субъектами цифровой экономики, в том числе по открытым телекоммуникационным сетям. Приведен краткий обзор средств и методов обеспечения защиты данных в телекоммуникационных сетях. Задача обеспечения сохранности цифровых данных при передаче определена как задача оптимального управления в условиях параметрических возмущений в неустойчивой среде. Выполнена формальная постановка задачи обеспечения сохранности цифровых данных при передаче по телекоммуникационным сетям. Показано, что для обеспечения сохранности при передаче цифровых данных в открытых телекоммуникационных сетях возможно использование технологий распределенных реестров. Кратко сформулированы возможные области применения решения задачи сохранности цифровых данных при передаче.

Ключевые слова: *цифровая экономика, сохранность, большие данные, распределенные реестры, персональные данные, электронные документы, оптимальное управление, параметрические возмущения.*

DOI: 10.14357/20790279190207

Введение

Стремительное движение к цифровой экономике порождает все новые научно-технические проблемы и вызовы. Цифровую экономику можно определить как экономическую деятельность, основой которой являются цифровые технологии и данные в цифровой форме. В узком смысле – это производство электронным бизнесом и электронной коммерцией электронных товаров и услуг. В более широком смысле цифровая экономика затрагивает практически все области обычной экономики, например, банковское дело, образование, здравоохранение. В еще более широком смысле – это некоторая сверхбольшая информационная система (ИС), представляющая собой Электронное государство и/или Электронное правительство, включающее управление экономической деятельностью с помощью цифровой платформы. Согласно программе цифровой экономики РФ [1], «данные в цифровой форме» становятся не просто хранимыми в защищенных средах данными, а «ключевым фактором производства во всех сферах социально-экономической деятельности». Это означает, что при взаимодействии различных субъектов цифровой экономики (производств, органов власти, граждан, медицинских и страховых учреждений, банков и т.д.) обмен информацией будет производиться именно в цифровой форме – цифровыми данными. Но, поскольку эти данные теперь являются ключевым фактором, то необходимо обе-

* Работа выполнена при частичной финансовой поддержке РФФИ в рамках научных проектов № 18-29-03070 и № 18-29-03085.

спечить их безопасную передачу, защиту от искажений и потерь, в том числе по открытым каналам связи и общим сетям (Интернет, мобильная связь) т.к. потеря этих данных приведет к огромным экономическим и репутационным потерям.

Тем самым, возникает противоречивая ситуация, в которой с одной стороны цифровые данные должны быстро, безопасно и открыто (в смысле того, что факт передачи должен быть виден всем абонентам конкретного информационного взаимодействия) передаваться между хозяйствующими субъектами цифровой экономики, с другой – должна быть обеспечена их сохранность при передаче. Под сохранностью будем понимать комплексное свойство цифровых данных существовать в качестве доступного, интерпретируемого (как в смысле возможности раскодирования и отображения, так и в смысле отсутствия потери семантики) и аутентичного (неискаженного) свидетельства (доказательства) в произвольный момент времени.

Описанная противоречивая ситуация порождает необходимость решения комплексной научно-технической проблемы обеспечения сохранности цифровых данных при передаче их по телекоммуникационным сетям между хозяйствующими субъектами в цифровой экономике, обеспечивая при этом разграничение доступа к данным и защиту конфиденциальных (в том числе персональных) данных.

1. Основные понятия и определения

Цифровая экономика – экономическая деятельность, основой которой являются цифровые технологии и данные в цифровой форме.

Штамп времени – это электронная подпись, установкой которой на электронном документе Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции этого документа. Т.е. дополнительное подтверждение аутентичности документа на указанный момент времени.

Служба штампов времени – это компонент программного обеспечения, который позволяет создавать доказательство факта существования некоторого электронного документа на определенный момент времени.

Большие данные (*big data*) – обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия.

Распределенный реестр – база данных, которая распределена между несколькими узлами телекоммуникационной сети. Каждый узел хранит полную копию реестра. Отсутствует единый центр управления. Каждый узел, независимо от других узлов, выполняет обновления реестра. Достижение согласия в отношении одной из копий реестра называется консенсусом (алгоритм выполняется автоматически всеми узлами реестра). Как только консенсус достигнут, распределенный реестр обновляется. Согласованная версия реестра сохраняется в каждом узле.

Блокчейн (*blockchain*) – технология, реализующая идею распределенных реестров или «выстроенная по определенным правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Чаще всего, копии цепочек блоков хранятся и независимо друг от друга (чрезвычайно параллельно) и обрабатываются на множестве разных компьютеров» [2].

Шардинг – это техника масштабирования работы с данными. Суть его в разделении базы данных на отдельные части так, чтобы каждую из них можно было вынести на отдельный сервер.

2. Обзор проблемы и решений

Попытки решения описанной проблемы активно предпринимаются. Для подтверждения актуальности поставленной проблемы, а также определения факторов, препятствующих ее решению, проведем краткий обзор различных способов защиты данных при передаче по телекоммуникационным сетям.

В настоящее время хорошо известны многие способы защиты телекоммуникационных сетей. В случае передачи данных по телекоммуникационным сетям общего пользования всегда предполагается, что передача не является безопасной. Для защиты данных разработаны несколько методов защиты, которые приняты во всем мире и хорошо известны. Методы защиты данных можно условно разделить на три класса [3-8]:

- на канальном уровне (например, с помощью протоколов PPTP (Point-to-Point Tunneling Protocol) или L2TP (Layer-2 Tunneling Protocol)[3]);
- на сетевом уровне (например, с помощью сетевых моделей OSI (open systems interconnection basic reference model) архитектуры и протоколов IPSec (Internet Protocol Security)[4]);
- на прикладном уровне (например, с помощью протоколов SSL (Secure Socket Layer)[5, 7], TLS (Transport Layer Security)[5, 6], SSH (Secure Shell) [8]).

Все три класса методов применимы и эффективны. Однако существуют три существенных не-

достатка для их использования в условиях цифровой экономики в РФ.

1. Реализации данных методов защиты, как правило, импортные, что в условиях экономических санкций против РФ создает реальную угрозу невозможности использования.
2. Многие реализации указанных методов защиты требуют постоянного обновления (фактически покупки) сертификатов, что опять же в условиях экономических санкций против РФ создает угрозу невозможности использования.
3. Ни одна из известных реализаций методов защиты не обеспечивает деперсонализацию цифровых данных, которая может потребоваться для обеспечения конфиденциальности персональных данных при передаче. Деперсонализацию можно определить так: представление персональных и/или конфиденциальных данных в виде, не позволяющем восстановить какую-либо информацию о субъекте персональных данных (определение дано по №152 ФЗ «О персональных данных» от 26.07.2006 г., в нем существует термин «обезличивание – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту»).

Ниже перечислены наиболее значимые стандарты, касающиеся безопасности ИС и телекоммуникационных сетей:

- Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем»;
- международный стандарт «Критерии оценки безопасности информационных технологий»;
- Федеральный стандарт США «Требования безопасности для криптографических модулей»;
- стандарты Internet-сообщества: «Руководство по информационной безопасности предприятия», «Как выбирать поставщика Интернет-услуг», «Как реагировать на нарушения информационной безопасности»;
- спецификации X.800 «Архитектура безопасности для взаимодействия открытых систем», X.500 «Служба директорий: обзор концепций, моделей и сервисов» и X.509 «Служба директорий: каркасы сертификатов открытых ключей и атрибутов»;
- стандарт BS 7799 «Управление информационной безопасностью. Практические правила» (ставший международным стандартом ISO/IEC 17799).

Как было показано в работах [9–11], цифровые данные в условиях цифровой экономики оказываются распределены между узлами территориально-распределенных больших ИС, охватывающих группы организаций или целые отрасли промышленности. В этих условиях можно говорить о применимости технологий распределенных реестров для обеспечения сохранности цифровых данных. Тем более, что они прямо определены программой цифровой экономики РФ [1] как одни из основных, наряду с большими данными и искусственным интеллектом.

В связи со стремительной «цифровизацией» прослеживается тенденция к распространению систем распределенного хранения данных. Создаются системы, позволяющие обеспечивать передачу распределенных данных. Как правило, большинство из них связано с технологиями блокчейн [14], которые, в свою очередь, являются реализациями технологий распределенных реестров.

Проще всего для организации обмена цифровыми данными в цифровой экономике создать отдельную, внешнюю по отношению ко всем участникам обмена, базу данных или управляющую ИС. Но создание такой системы требует невероятно больших организационных и финансовых затрат. Кроме того, выход из строя управляющего центра ИС парализовал бы экономику в целом. Также до недавнего времени такое решение имело ряд технических ограничений, связанных с отсутствием доверенных СУБД, способных, с одной стороны, обеспечивать защищенное распределенное хранение больших данных, с другой, многопользовательский режим работы.

Появление распределенных параллельных СУБД [12] обеспечило относительно недорогое хранение данных и прозрачный перенос данных между узлами телекоммуникационной сети. Перенос был обеспечен за счет механизмов репликации, а также вертикального и горизонтального шардинга. Несмотря на явный прогресс, применение таких СУБД в цифровой экономике РФ под большим вопросом из-за отсутствия аналогичных отечественных решений, а также из-за того, что такие СУБД сами по себе не решают проблемы аутентичности, разграничения доступа.

Появление первых относительно безопасных реализаций распределенных реестров цифровых данных связано с возникновением программных реализаций штампов времени в 1990-е годы. Они

позволяли осуществлять сбор транзакций в блоки и связывать их при помощи хеш-функций.

Развитие этого подхода в 2000-х годах привело к созданию блокчейн-технологий. В их реализациях к принципу хранения связанных штампов времени было добавлено применение современных средств шифрования и хэширования, а так же введение специальных узлов (майнеров), которые занимаются регистрацией транзакций в общей телекоммуникационной сети, используя предназначенные для этого алгоритмы консенсуса, которые должны гарантировать аутентичность цифровых данных. В это же время начинается активное развитие технологий распределенных вычислений, позволяющих создавать сети из недорогих компьютеров, устойчивые к выведению узлов из строя.

Многочисленные реализации технологий блокчейн, в первую очередь, при создании криптовалют, различаются размерами и структурой регистрируемых блоков, применением различных алгоритмов консенсуса для организации работы сети [14].

Рассмотрим примеры реализаций защищенного обмена цифровыми данными.

Проект Peppol – ИС обмена электронными документами между представителями государств Европейского Союза (ЕС) и их контрагентами. Проект был создан в рамках инициатив ЕС. В каждой стране ЕС существует авторизованный Peppol – оператор, который осуществляет прием сообщений от других авторизованных операторов (не только из стран ЕС), и перенаправляет их конечным организациям. Внутри Peppol существует согласованный формат обмена цифровыми данными, стандарт шифрования, используется инфраструктура центров сертификации [15].

В РФ примером системы обмена цифровыми данными является российская система Межведомственного электронного документооборота (МЭДО), которая обеспечивает обмен между государственными органами и Система межведомственного электронного взаимодействия (СМЭВ), которая обеспечивает гражданам РФ доступ к услугам в электронной форме через портал государственных услуг РФ.

При рассмотрении этих систем, в первую очередь необходимо отметить, что в ИС Peppol и МЭДО/СМЭВ обмен цифровыми данными выполняется специализированными организациями (операторами). Они же являются регуляторами этого обмена, устанавливают форматы и требования информационной безопасности обмена данными. Тем самым, риск нарушения аутентичности передаваемых данных находится на том же уровне, что и в случае традиционных систем с централизованным хранением данных. Не рассматривается проблема деперсонализации данных, универсального законченного программно-технического решения также не видно.

Отсутствие универсального решения связано с несколькими факторами:

- проблема обмена цифровыми данными не является чисто технической. Существует необходимость решать организационные, юридические вопросы, связанные с необходимостью или возможностью передачи персональных, конфиденциальных, секретных данных, с использованием средств криптографической защиты информации, разработки правил, нормативных документов и организационных мер обеспечения обмена данными;
- цифровая экономика только начинает развиваться, вследствие чего отсутствует системный подход к проблемам обмена данными, который не сводится только к обеспечению безопасности каналов связи, или проставлению «галочки» «согласен на то, что мои персональные данные будут переданы по открытым каналам связи» но и затрагивает проблемы обеспечения аутентичности, деперсонализации, прозрачности и надежности обмена цифровыми данными для участников информационного взаимодействия в рамках цифровой экономики;
- отсутствует методология контроля параметров программно-аппаратной среды обмена цифровыми данными;
- не все проблемы обмена цифровыми данными до конца изучены и систематизированы.

Из краткого обзора проблемы сохранности при передаче цифровых данных видно, что поставленная проблема является актуальной и находится в русле общемировых тенденций.

3. Обзор проблем сохранности цифровых данных при передаче

Прежде чем перейти к формальной постановке задачи сохранности цифровых данных при их передаче между хозяйствующими субъектами цифровой экономики приведем обзор возникающих рисков.

Во-первых, риск нарушения ***аутентичности*** цифровых данных в процессе передачи. Он может возникнуть по причине намеренного или случайного искажения или удаления данных вследствие несанкционированного доступа (НСД).

Во-вторых, риск нарушения ***интерпретируемости*** цифровых данных. Зависимость от конкретного формата цифровых данных, протоколов пере-

дачи данных, формата кодирования и алгоритмов шифрования и дешифрации, которые со временем могут перестать поддерживаться, а также от средств отображения данных, может привести к тому, что цифровые данные превратятся в бессмысленную бинарную последовательность «нулей» и «единиц», расшифровка которой станет невозможной.

В-третьих, риск потери ***семантики*** данных. Цифровые данные привязаны к некоторым метаданным, которые описывают их и определяют их смысл. Например, есть разница в передаче данных «45000» и «Зарплата 45000 рублей». Во втором случае назначение данных понятно. Данные могут передавать и в первом виде, но тогда в узлах ИС на концах телекоммуникационной сети должны быть однозначно определены схемы данных, порядок их передачи и т.д. Иначе потеря метаданных критическим образом скажутся на возможности их использовать.

В-четвертых, риск нарушения ***надежности*** передачи цифровых данных. Если рассматривать этот риск шире, то это риск нарушения надежности конкретных программно-технических средств телекоммуникационных сетей.

В-пятых, риск нарушения ***устойчивости*** программно-технических средств телекоммуникационных сетей к внешним воздействиям, в том числе и катастрофического характера. Риск нарушения устойчивости выделен отдельно от риска нарушения надежности, т.к. программно-технические средства могут работать надежно, но при этом быть выведены из строя воздействиями катастрофического характера, в том числе вследствие нарушения информационной безопасности или человеческого фактора.

И, наконец, это риск передачи персональных и/или конфиденциальных данных в ситуации, когда это запрещено.

Если для обеспечения аутентичности цифровых данных при передаче используются технологии распределенных реестров, то по отношению к ним также можно рассматривать воздействие всех перечисленных рисков, кроме риска передачи конфиденциальных и персональных данных, т.к. они лишь фиксируют факт передачи. Однако для технологий распределенных реестров появляется еще один риск. Так как хранение информации о фактах передачи цифровых данных является уже задачей обеспечения долговременной сохранности [9], то при обеспечении долговременной сохранности данных возникает дополнительный риск – зависимость от конкретных технических и программных средств криптографической защиты и средств хранения распределенных блоков. Ведь технологии распределенных реестров, как любые цифровые технологии, реализованы с помощью конкретных программно-технических средств [2, 11, 14], а в случае потери или искажения данных нужно будет провести расследование о существовании факта передачи.

4. Постановка задачи обеспечения сохранности цифровых данных при передаче

Если суммировать обзор проблем сохранности передачи цифровых данных, то можно сделать следующий вывод. Сохранность, как комплексное свойство, включающее аутентичность, интерпретируемость, надежность, устойчивость, сохранение семантики данных должна обеспечиваться независимо от протоколов, форматов, программных и технических средств передачи данных. В этом случае можно представить цифровые данные как объект управления, а телекоммуникационные сети как нестабильную среду передачи цифровых данных.

Тогда цифровые данные – это объект управления. Задача обеспечения сохранности цифровых данных при передаче – это задача оптимального управления цифровыми данными в условиях параметрических возмущений цифровой программно-технической среды хранения цифровых данных, также как и задача долговременной сохранности [9]. Для оптимального управления необходимо контролировать параметры среды передачи цифровых данных, т.е. разработать математические модели и алгоритмы контроля.

Если в обеспечении сохранности передачи данных участвуют программные и технические средства, реализованные по технологиям распределенных реестров, то математическая постановка задачи возможна в следующем виде:

1) Множество данных в цифровой форме $\boldsymbol{Didf} = \{ \boldsymbol{didf}_i \}$;
2) Множество блоков распределенных реестров $\boldsymbol{Bch} = \{ \boldsymbol{bch}_j \}$;
3) Множество параметрических возмущений среды хранения $\boldsymbol{E} = \{ \varepsilon_q \}$:
   - ε_1 – нарушение аутентичности ***Didf***, ***Bch***,
   - ε_2 – нарушение интерпретируемости ***Didf***, ***Bch***,
   - ε_3 – нарушение семантики ***Didf***, ***Bch***,
   - ε_4 – нарушение надежности передачи ***Didf***, и хранения ***Bch***,
   - ε_5 – нарушение устойчивости ***Didf***, ***Bch***,
   - ε_6 – нарушение независимости ***Bch***;
4) Исходный уровень сохранности для ***Didf***, ***Bch*** – $\boldsymbol{SV}_0$.

Найти: Множество математических моделей $\mu = \{ \mu_r \}$, контроля параметров сохранности (включая аутентичность, интерпретируемость, со-

хранение семантики, надежность, устойчивость, независимость ***Bch***) при обмене ***Didf*** между ИС.

Для контроля параметров сохранности при передаче необходима разработка математических моделей. Тогда задача контроля сохранности цифровых данных при передаче представляет собой задачу оптимального выбора по многим критериям.

Действительно, пусть сохранность цифровых данных $didf_i$ при передаче характеризуется функцией $\mu(t)$, значение которой представляет собой вероятность сохранности цифровых данных $didf_i$ при передаче на уровне SV_0 в произвольный момент времени t. Тогда можно утверждать, что задача обеспечения сохранности цифровых данных $didf_i$ при передаче формулируется, как задача достижения максимума функции $\mu(t)$ на произвольном временном интервале t. Т.е.: $M = \max_{t \in [t0,\infty]} \mu(t)$, где $t0$ – момент времени начала передачи $didf_i$, тогда

$$\mu(t) = \min(\alpha_d(t)^{\omega 1} \zeta_d(t)^{\omega 2} \sigma_d(t)^{\omega 3} \rho_d(t)^{\omega 4} \varphi_d(t)^{\omega 5} (1 - \psi_d(t))^{\omega 6},$$
$$\alpha_b(t)^{\omega 7} \zeta_b(t)^{\omega 8} \sigma_b(t)^{\omega 9} \rho_b(t)^{\omega 10} \varphi_b(t)^{\omega 11} (1 - \varsigma_b(t))^{\omega 12}),$$

где ω_i – назначаемые экспертами коэффициенты важности соответствующих показателей $\sum \omega_i = 1$; $\omega_i > 0$, i=[1,6] и $\sum \omega_i = 1$, $\omega_i > 0$, i=[7,12];

$\alpha_d(t)$, $\alpha_b(t)$ – вероятности сохранения аутентичности соответственно для ***Didf*** и ***Bch*** на произвольном временном интервале t;

$\zeta_d(t)$, $\zeta_b(t)$ – вероятности интерпретируемости соответственно для ***Didf*** и ***Bch*** на произвольном временном интервале t;

$\sigma_d(t)$, $\sigma_b(t)$ – вероятности сохранения семантики соответственно для ***Didf*** и ***Bch*** на произвольном временном интервале t;

$\rho_d(t)$, $\rho_b(t)$ – надежность хранения соответственно для ***Didf*** и ***Bch*** на произвольном временном интервале t;

$\varphi_d(t)$, $\varphi_b(t)$ – вероятности сохранения устойчивости соответственно для ***Didf*** и ***Bch*** на произвольном временном интервале t;

$\psi_d(t)$ - вероятность передачи персональных данных ***Didf*** при запрете на такую передачу или вероятность потери (кражи) персональных данных при передаче на произвольном временном интервале t;

$\varsigma_b(t)$ – вероятность зависимости ***Bch*** от конкретной реализации и программно-технических и криптографических средств на произвольном временном интервале t.

Для каждого параметра должны быть разработаны свои математические модели. В дальнейших статьях авторов будет приведена их разработка.

5. Возможное практическое применение математических моделей

Конечно, математические модели контроля параметров сохранности цифровых данных при передаче не решают проблему сохранности. Однако они могут стать неотъемлемой частью технологии обеспечения сохранности цифровых данных при передаче. Возможные практические применения данной технологии, предполагающей деперсонализацию данных или защищенную передачу персональных данных следующие:

- Защищенная передача медицинских данных (например, медицинских карт, анализов и прочее). Задача очень актуальна в связи с вводом генетических паспортов, сбора биометрических данных, да и просто перевода из одного медицинского учреждения в другое.
- Передача данных отделов кадров при переходе на другую работу.
- Передача персональных данных и данных о заработке между БД государственных и негосударственных Пенсионных фондов, при смене региона проживание и трудовой деятельности.
- Обезличивание данных при передаче в процессе проведении выборов в системах электронного голосования.

В условиях развивающейся цифровой экономики могут быть и другие применения.

Наиболее предпочтительным методом обезличивания представляется метод введения идентификаторов, предполагающий замену фамилий и имен субъектов условными идентификаторами с передачей таблицы соответствия этих идентификаторов реальным субъектам отдельно от основного массива информации.

Заключение

В данной статье проведена систематизация проблем обеспечения сохранности цифровых данных при их передаче между информационными системами по телекоммуникационным сетям. Показана актуальность решения данной задачи в условиях цифровой экономики. Представлена формальная постановка задачи обеспечения сохранности цифровых данных при передаче как задача оптимального управления объектом хранения в условиях параметрических возмущений программно-технической среды. Результатом решения задачи должна стать технология, представляющая собой совокупность математических моделей, алгоритмов и программно-технических решений для обеспечения сохранности данных в цифровой форме при передаче. Обозначен круг возможного практического применения решения задачи. В следующих статьях планируется привести разработку математических моделей контроля параметров среды передачи цифровых данных.

Литература

1. *Программа* «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. М.:2017 – 88 с.
2. *Melanie Swan*. Blockchain: Blueprint for a New Economy. – O'Reilly Media, Inc., 2015. – 152 p. В русском переводе Мелани Свон. Блокчейн: Схема новой экономики. – Олимп-Бизнес, 2016. – 240 с.
3. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012.-592с
4. *IPSec* – протокол защиты сетевого трафика на IP-уровне [Электронный ресурс] – iXBT.com – Режим доступа: http://www.ixbt.com/comm/ipsecure.shtml (дата обращения: 03.04.2019).
5. *Rescorla Eric.* SSL and TLS: Designing and Building Secure Systems. – 1-st. – Addison-Wesley Professional, October 27, 2000. – T. 1. – 528 p.
6. *Dierks T., Rescorla E.* The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008
7. *Freier A., Karlton P., Kocher P.* The Secure Sockets Layer (SSL) Protocol Version 3.0, RFC 6101, August 2011.
8. *Stephen C. Williams*. Analysis of the SSH Key Exchange Protocol, 2017.
9. *Соловьев А.В., Баканова Н.Б.* Проблемы долговременной сохранности больших данных // Информационные технологии и вычислительные системы, 2019, №2 (в печати).
10. *Акимова Г.П., Даниленко А.Ю., Пашкина Е.В., Пашкин М.А., Соловьев А.В., Тарханов И.А.* Применение технологии блокчейн в информационных системах. Часть 3. Цифровая экономика и сохранность электронных документов. // Системы высокой доступности. 2018. Т. 14. № 1. С. 13–19.
11. *Даниленко А.Ю., Акимова Г.П.* Особенности применения технологии блокчейн // Материалы 27-й научно-технической конференции Методы и технические средства обеспечения безопасности информации 24-27 сентября 2018 года. СПб: Издательство политехнического университета. 2018. С. 73–75.
12. *Valduries P.* Parallel Database Systems: Open Problems and New Issues. Distributed and Parallel Databases, April 1993, 1(2), pp. 137-165.
13. *Haber S., Stornetta W.S.* (1991). «How to time-stamp a digital document». Journal of Cryptology. 3 (2). doi:10.1007/BF00196791
14. *Anderson L., Holz R., Ponomarev A., Rimba P., & Weber I.* (2016). New kids on the block: an analysis of modern blockchains.
15. *OpenPeppol*. Transport Infrastructure ICT Services-Components. Trust Network Certificate Policy. [Электронный ресурс] Version: 2.00. 07.07.2014. Режим доступа: https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-Trust_Network_Certificate_Policy-2.00.pdf
16. *Соловьев А.В., Тарханов И.А.* Электронные документы и задача обеспечения сохранности при обмене данными в цифровой экономике // Труды ИСА РАН, Т. 68. Вып. 1. 2018. С.42-53. DOI 10.14357/20790279180104.
17. *Akimova G.P., Solovyev A.V., Tarkhanov I.A.* Reliability Assessment Method for Geographically Distributed Information Systems // The IEEE 12th International Conference on Application of Information and Communication Technologies / AICT 2018 (17-19 Oct. 2018, Almaty, Kazakhstan), IEEE, 2018, P.188-191.

Соловьев Александр Владимирович. Институт системного анализа Федерального исследовательского центра «Информация и управление» РАН (ИСА ФИЦ ИУ РАН). Главный научный сотрудник. Доктор технических наук. Количество печатных работ: 90. Область научных интересов: системный анализ, системы управления базами данных, теория надежности, математическое моделирование, долговременное хранение электронных документов. E-mail: soloviev@isa.ru

Даниленко Андрей Юрьевич. ИСА ФИЦ ИУ РАН. Ведущий научный сотрудник. Кандидат физико-математических наук. Количество печатных работ: 35. Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru

Акимова Галина Павловна. ИСА ФИЦ ИУ РАН. Ведущий научный сотрудник. Кандидат технических наук. Количество печатных работ: 60. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Богданов Дмитрий Степанович. ИСА ФИЦ ИУ РАН. Старший научный сотрудник. Кандидат технических наук. Количество печатных работ: 33. Область научных интересов: системный анализ, системы управления базами данных, распознавание образов, распознавание речи, электронные архивы. E-mail: bogdanov@isa.ru

Пашкин Матвей Александрович. ИСА ФИЦ ИУ РАН. Научный сотрудник. Количество печатных работ: 20. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: pashkin@isa.ru

Пашкина Елена Владимировна. ИСА ФИЦ ИУ РАН. Ведущий программист. Количество печатных работ: 20. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Подрабинович Андрей Александрович. ИСА ФИЦ ИУ РАН. Ведущий программист. Количество печатных работ: 10. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации. E-mail: andy_eup@mail.ru

Туманова Ирина Владимировна. ИСА ФИЦ ИУ РАН. Ведущий программист. Количество печатных работ: 5. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: tumanova-irin@mail.ru

Mathematical models for assessing the integrity of digital data transfer in a digital economy

A.V. Solovyev[I], A.Yu. Danilenko[I], G.P. Akimova[I], D.S. Bogdanov[I], M.A. Pashkin[I], E.V. Pashkina[I], A.A. Podrabinovich[I], I.V. Tumanova[I]

[1] Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia

Abstract. This article describes mathematical models for assessing the integrity of digital data when they are transmitted between economic entities of the digital economy, including through open telecommunications networks. The paper provides a brief overview of the means and methods of ensuring data protection in telecommunications networks. The classification of the problem of ensuring the preservation of digital data as an optimal control problem under parametric perturbations in an unstable environment has been made. A formal formulation of the task of ensuring the safety of digital data during transmission over telecommunication networks has been completed. It is shown that to ensure the safety of digital data transmission in open telecommunications networks, it is possible to use distributed registry technologies. The possible areas of application of the solution of the problem of preserving digital data during transmission are outlined.

Keywords: *digital economy, safety, big data, distributed registries, personal data, electronic documents, optimal control, parametric perturbations*

DOI: 10.14357/20790279190207

References

1. *Program* "Digital Economy of the Russian Federation". APPROVED by the order of the Government of the Russian Federation at July 28, 2017. № 1632-r. M.:2017 – 88 p.
2. *Melanie Swan.* Blockchain: Blueprint for a New Economy. – O'Reilly Media, Inc., 2015. – 152 p.
3. *Shan'gin V.F.* Zastshita informacii v kompyuternyh systemah I setyah [Information security in computer systems and networks] Moscow: DMK Press, 2012.-592p.
4. *IPSec* – protocol zastshity setevogo trafika na IP-urovne [protocol for network traffic protection at the IP level] [Electronic resource] – iXBT.com – Access mode: http://www.ixbt.com/comm/ipsecure.shtml (03.04.2019).
5. *Rescorla Eric*. SSL and TLS: Designing and Building Secure Systems. – 1-st. – Addison-Wesley Professional, October 27, 2000. – T. 1. – 528 p.
6. *Dierks T., Rescorla E.* The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August. 2008
7. *Freier A., Karlton P., Kocher P.* The Secure Sockets Layer (SSL) Protocol Version 3.0, RFC 6101, August 2011.

8. *Stephen C. Williams*. Analysis of the SSH Key Exchange Protocol, 2017.
9. *Solovyev A.V., Bakanova N.B.* Problemy dolgovremennoy sohrannosti bolshih dannih [Problems of long-term preservation of big data] // Informacionniye tehnologii I vychislitel'niye systemy [Information technology and computing systems], №2, 2019 (in print).
10. *Akimova G.P., Danilenko A.Yu., Pashkina E.V., Pashkin M.A., Solovyev A.V., Tarkhanov I.A.* Primeneiye tehnologii blockchain v informacionnih systemah. Chast' 3. Cifrovaya ekonomika I sohrannost' elektronnih dokumentov [The use of blockchain technology in information systems. Part 3. The digital economy and the preservation of electronic documents] // Systemy visokoy dostupnosti [High Availability Systems]. 2018. T. 14. № 1. P. 13–19.
11. *Danilenko A.Yu., Akimova G.P.* Osobennosti primeneniya tehnologii blockchain [Features of blockchain technology] // Materialy 27 nauchno-tehnicheskoy konferencii "Metody i tehnicheskiye sredstva obespecheniya bezopasnosti informacii" [Materials of the 27th Scientific and Technical Conference Methods and Technical Means for Information Security] 24-27 september 2018. S-Pb: Izdatelstvo politehnicheskogo universiteta [Publishing house of the Polytechnic University]. 2018. P. 73–75.
12. *Valduries P.* Parallel Database Systems: Open Problems and New Issues. Distributed and Parallel Databases, April 1993, 1(2), pp. 137-165.
13. *Haber S.; Stornetta W. S.* (1991). «How to timestamp a digital document». Journal of Cryptology. 3 (2).
14. *Anderson L., Holz R., Ponomarev A., Rimba P., & Weber I.* (2016). New kids on the block: an analysis of modern blockchains (2016).
15. *OpenPeppol*. Transport Infrastructure ICT Services-Components. Trust Network Certificate Policy. [Electronic resource] Version: 2.00. 07.07.2014. Access mode: https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-Trust_Network_Certificate_Policy-2.00.pdf
16. *Solovyev A.V., Tarkhanov I.A.* Elektronniye dokumenty i zadacha obespecheniya sohrannosti pri obmene dannymi v cifrovoy ekonomike [Electronic Documents and the Security Challenge of Data Interchange in the Digital Economy] // Trudy Instituta systemnogo analiza RAN [Proceedings of the Institute for System Analysis of the Russian Academy of Sciences (ISA RAS)], Tom 68, issue 1, M.: 2018. P.42-53.
17. *Akimova G.P., Solovyev A.V., Tarkhanov I.A.* Reliability Assessment Method for Geographically Distributed Information Systems // The IEEE 12th International Conference on Application of Information and Communication Technologies / AICT 2018 (17-19 Oct. 2018, Almaty, Kazakhstan), IEEE, 2018, P.188-191.

Solovyev A.V. Chief Researcher, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Doctor of Technical Sciences. Number of publications: 88. Area of scientific interests: system analysis, database management systems, reliability theory, mathematical modeling, electronic document management, electronic archive, long-term storage of electronic documents. E-mail: soloviev@isa.ru

Danilenko A.Yu. Leading Researcher, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Candidate of Physical and Mathematical Sciences. Number of publications: 35. Area of scientific interests: system programming, system analysis, information technology, electronic document management, information security, data protection. E-mail: danilenko@isa.ru

Akimova G.P. Leading Researcher, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Candidate of Technical Sciences. Number of publications: 60. Area of scientific interests: system programming, system analysis, information technologies, the influence of the human factor, information and analytical systems, electronic document management, electronic archive. E-mail: akimova@isa.ru

Bogdanov D.S. Senior Research fellow, Department 93 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Candidate of Technical Sciences. Number of publications: 33. Area of scientific interests: system analysis, database management systems, pattern recognition, speech recognition, electronic archives. E-mail: bogdanov@isa.ru

Pashkin M.A. Researcher, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Number of publications: 20. Area of scientific interests: system programming, information technologies, information and analytical systems, electronic archive. E-mail: pashkin@isa.ru

Pashkina E.V. lead programmer, Department 91 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Number of publications: 20. Area of scientific interests: system programming, information technology, electronic document management, electronic archive. E-mail: pashkina@isa.ru

Podrabinovich A.A. lead programmer, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Number of publications: 10. Area of scientific interests: system programming, design and creation of methods and software for managing electronic documents, information security. E-mail: andy_eup@mail.ru

Tumanova I.V. lead programmer, Department 94 ISA FRC CSC RAS. Moscow, prosp. 60-let Oktyabrya, 9. Number of publications: 5. Area of scientific interests: system programming, information technology, electronic document management, electronic archive. E-mail: tumanova-irin@mail.ru