

УДК 004.01

В. С. Костенков, В. В. Данилов, Н. А. Тимошенко
Донецкий национальный университет, Донецк

ОСОБЕННОСТИ ПОСТРОЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В КОНТЕКСТЕ ПРОВЕРКИ ПОДЛИННОСТИ ДОКУМЕНТОВ

В данной статье приводится анализ эффективности использования электронной цифровой подписи в Российской Федерации при проверке подлинности документов. Проанализированы преимущества и недостатки различных технологий обработки информации при построении единой информационной системы. Данная система рассматривается авторами как альтернативный подход по обеспечению контроля подлинности документов.

Ключевые слова: информационные системы; технологии обработки информации; подлинность документов; электронная цифровая подпись; мошенничество.

V.S. Kostenkov, V.V. Danilov, N.A. Timoshenko
Donetsk National University, Donetsk

FEATURES OF CONSTRUCTION OF INFORMATION SYSTEMS IN THE CONTEXT OF CHECKING THE AUTHENTICITY OF DOCUMENTS

This article provides an analysis of the effectiveness of using an electronic digital signature in the Russian Federation when verifying the authenticity of documents. The advantages and disadvantages of various information processing technologies in the construction of a unified information system are analyzed. This system is considered by the authors as an alternative approach to ensure control of the authenticity of documents.

Keywords: information systems; information processing technologies; document features; electronic digital signature; fraud.

Постановка проблемы. Эффективность эксплуатации систем электронного документооборота во многом зависит от совершенствования механизмов по обеспечению информационной безопасности. Важную роль в подобных системах занимает процедура электронной цифровой подписи (далее - ЭЦП). Она ориентирована на подтверждение авторства того или иного электронного документа с помощью криптографических методов. Однако, в связи с участвовавшими фактами мошенничества в сфере ЭЦП [1-3] актуальность приобретают вопросы не отдельного использования процедуры цифровой подписи, а разработки специализированной информационной системы (далее – ИС) по обеспечению проверки подлинности документов.

Анализ исследований. Исследованием вопросов, связанных с построением систем по контролю подлинности документов, занимались учёные: Моисеева Т.Ф., Вострецова Е. В., Хачатурова С. С. [4] и другие. Вместе с тем, многоаспектность проблем, касающихся разработки информационных систем в контексте проверки подлинности документов, обуславливает насущную потребность в дальнейших исследованиях по данному направлению.

Целью данной работы выступает исследование и обобщение научных положений о построении информационных систем по проверке подлинности документов. В соответствии с поставленной целью, необходимо решить следующие задачи: 1) анализ тенденций развития электронной цифровой подписи; 2) анализ тенденций развития информационных систем; 3) разработка возможных направлений развития при построении информационных систем в контексте проверки подлинности документов.

Основной материал. Основным стимулом к написанию данной статьи послужила публикация новостного агентства РБК [5] информации о планах правительства РФ о запуске масштабного эксперимента по выдаче облачной ЭЦП. Как отмечает представитель Минкомсвязи, программа рассчитана на два года, и проект постановления правительства на момент написания статьи находится в стадии обсуждения с заинтересованными ведомствами.

В указанной программе разработан порядок выдачи и контроля за использованием электронной цифровой подписи. Отмечается, что цифровая подпись выдается после процедуры авторизации в одной из следующих автоматизированных информационных системах:

1. Единой системе идентификации и аутентификации (далее – ЕСИА);
2. Единой биометрической системе.

Комбинированное использование двух упомянутых систем применяется банками для оформления процедуры удаленного управления вкладами. Представители компании Cisco Systems отмечают, что основным преимуществом разрабатываемой облачной ЭЦП является отсутствие необходимости использования на стороне пользователей специализированного настольного программного обеспечения (далее – ПО). В свою очередь, это исключает возможность утери компонентов, необходимых для формирования ЭЦП, которые хранятся на съемных носителях информации. Авторами данной программы отмечается, что распространение усиленной квалифицированной цифровой подписи предоставит возможность удаленного проведения юридических операций по присвоению или отчуждению каких-либо прав между организациями и гражданами. Разрабатываемый механизм предоставит широкие полномочия и станет аналогом собственноручной подписи. Типичными угрозами при использовании ЭЦП являются:

1. Оформление и подача документов на регистрацию сделок с недвижимостью в электронном виде. Вследствие незаконного использования ЭЦП пострадавшая сторона может лишиться как денег, так и жилплощади. Попадают в эту категорию: процедура дарения и купли-продажи.

2. Области кредитования. Мошенники оформляют на имя потерпевшего поддельные документы и получают деньги удалённым способом. Эта схема востребована в процессе оформления займов онлайн.

3. Регистрация бизнеса. В этом случае пострадавшая сторона может лишиться собственного дела или стать владельцем фирмы-однодневки. В результате владельца ЭЦП могут обвинить в "отмывании" денег если будет установлен данный состав преступления.

По состоянию на октябрь 2020 года, на территории Российской

Федерации действуют 506 аккредитованных удостоверяющих центров. Однако, с каждым годом увеличивается количество правонарушений с применением цифровых подписей, которые были выданы указанными центрами. Одним из преступлений, получившим огласку во втором полугодии 2020 года, является факт удаленной регистрации мошенниками таксопарка по реквизитам случайной компании [3]. Анализ приведенных ситуаций показывает, что основной причиной данных правонарушений являются недоработка нормативной правовой базы и проблема в разграничении прав доступа к информации. Более детальное изучение особенностей научно-технологического развития Российской Федерации в контексте проверки подлинности документов, их авторства и состояния законодательной базы РФ было проведено в статье [6].

В соответствии с федеральным законом РФ «Об информации, информационных технологиях и о защите информации», под понятием «информационная система» подразумевается некий, хранящийся в базе данных, объем данных, который обрабатывается с помощью специализированных технологий и технических средств. Когаловский М. Р. [7] в своей работе уточняет, что в понятие входят не только данные, но и: людские и информационные ресурсы, лингвистические средства, программно-аппаратное обеспечение и коммуникационное оборудование. Все это обеспечивает «динамичность информационной модели выбранной части реального мира». На наш взгляд, подобное понимание термина является достаточно широким и будет более целесообразным дать более узкую его трактовку. В ГОСТ Р 53622-2009 под ним подразумевается некий набор баз данных, системы управления и ПО, которые функционируют на вычислительных средствах как единое целое для выполнения определенной цели.

Подобная информационная система должна включать в себя специализированную подсистему, обеспечивающую непрерывное накопление данных о пользователях и истории их взаимодействий с различного рода документами. На основании анализа полученных данных представляется возможным обеспечить механизм неотказуемости от авторства. Данная подсистема может состоять из:

1. Периферийной части, сопровождающей пользователей в момент заключения электронных договоров. Подобное сопровождение может обеспечиваться с помощью централизованной, децентрализованной или распределенной обработок информации;

2. Базы данных, в которой производится накопление всех данных;

3. Дополнительной подпрограммы, обеспечивающей аналитическую обработку данных;

4. Операционной части, предоставляющей процедуры авторизации проводимых операций и оперативного взаимодействия с другими подсистемами;

5. Распределенной системы, обеспечивающей механизм синхронизации информации между подобными подсистемами. Примерами реализации подобной системы являются RAID технология и отечественная система

хранения данных TATLIN [8].

Централизованная система предполагает прямое взаимодействие множества клиентских узлов с определенным сервером. Преимуществами данной технологии являются: 1) простота в обслуживании вычислительной системы; 2) простота внедрения новых методологических решений. К недостаткам данной технологии относят: 1) низкая отказоустойчивость; 2) низкая производительность; 3) функциональная ограниченность. Указанные преимущества и недостатки такого типа систем влекут следующие ограничения: 1) сложность вертикального масштабирования; 2) наличие узких мест при увеличении нагрузки на информационную систему.

Децентрализованная технология предполагает независимость принятия решений на уровне узла системы. Конечное поведение всей системы зависит от общей согласованности между собой решений каждого узла. Преимуществами данной технологии являются: 1) низкая вероятность появления узких мест при увеличении нагрузки на информационную систему; 2) высокая доступность; 3) автономность работы отдельного узла. К недостаткам данной технологии относят: 1) отсутствие контролирующих узлов; 2) сложность общего обслуживания системы; 3) сложность прогнозирования поведения отдельного узла. Указанные преимущества и недостатки такого типа систем влекут следующие ограничения: 1) сложность в регулировании отдельного узла системы; 2) сложность в решении коллективной задачи.

Ключевыми преимуществами распределенной технологии обработки информации являются: 1) масштабируемость; 2) оперативность выполнения задач; 3) многопользовательский доступ к информационному ресурсу; 4) высокая отказоустойчивость; 5) функциональная дифференциация; 6) оптимизация затрат на аппаратное обеспечение. К недостаткам данной технологии относят: 1) сложность в координации решений, принимаемых узлами системы; 2) сложность регистрации событий, происходящих в системе. Указанные преимущества и недостатки такого типа систем влекут следующие ограничения: 1) сложность во внедрении и обслуживании алгоритмов. Данное ограничение связано с отсутствием общих часов между всеми элементами; 2) сложность в принятии обоснованного решения на уровне узла связи, в связи с отсутствием представлений о деятельности других узлов; 3) сложность упорядочивания проводимых транзакций между терминалами различных узлов связи. Связано с отсутствием общих часов между всеми элементами. В результате анализа преимуществ и недостатков технологий обработки информации наиболее приоритетным является комбинирование распределенного и централизованного типов систем. Каждый субъект информационной системы действует в соответствии с действующими полномочиями. Отметим, что более детальный анализ разрабатываемой информационной системы в статье не рассматривается.

Образующим элементом всей системы является сеть передачи данных (далее - СПД). Подобные СПД состоят из центрального узла (далее – ЦУ), узлов (далее – УС) и каналов связи. В задачи ЦУ входят: 1) разработка и совершенствование нормативной правовой основы деятельности субъектов

информационной системы; 2) контроль за выполнением нормативных документов; 3) организация и осуществление мер по предупреждению, пресечению, выявлению и устранению правонарушений в действующей информационной системе; 4) выявление и устранение нерегламентированных возможностей информационной системы; 5) координация действий между УС; б) распределение привилегий между всеми участниками информационной системы. В задачи УС входят: 1) прием и последующая передача пакетов в направлениях, которые обеспечивают оптимальную доставку данных; 2) контроль за выполнением нормативных документов; 3) организация и осуществление мер по предупреждению, пресечению, выявлению и устранению правонарушений в подотчетной системе. Совокупность объединенных сетью передачи данных локальных серверов (далее – ЛС), подключаемых к узлам связи, образуют сеть локальную вычислительную сеть. Множество терминалов (Т) и средств связи (далее – СС), обеспечивающих подключение терминалов к ЛС, образует терминальную сеть. Принципиальная схема информационной системы представлена на рисунке 1.

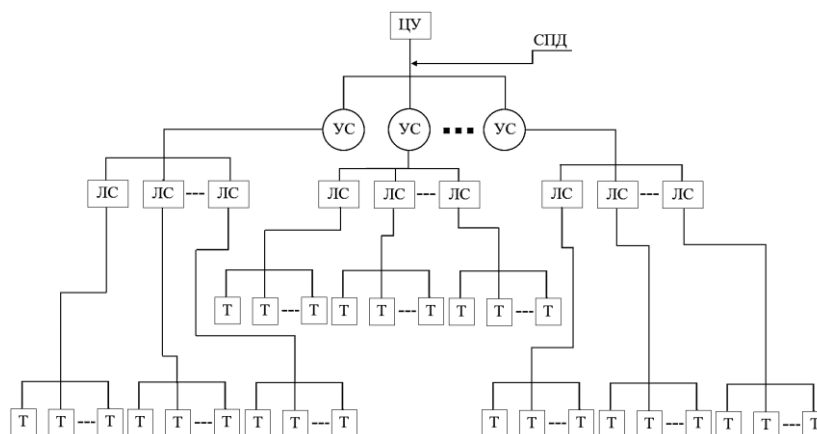


Рисунок 1 – Принципиальная схема информационной системы

Отметим, что пользовательское взаимодействие в данной информационной системе осуществляется с помощью электронно-вычислительных машин (далее – ЭВМ), подключаемых через общедоступные каналы связи. Данные передаются в форме блоков, в которых также содержится служебная информация, необходимая для управления процессами передачи и защиты данных.

Выводы: 1) Проведен анализ недостатков использования электронной цифровой подписи в Российской Федерации при проверке подлинности документов. 2) Исследованы преимущества и недостатки различных технологий обработки информации при построении единой информационной системы по проверке подлинности документов; 3) Предложен альтернативный подход к построению системы по контролю подлинности документов.

Список литературы

1. Новый вид мошенничества: Подделка электронной подписи [Электронный ресурс] // Комсомольская правда: Сетевое издание (сайт). URL: <https://www.donetsk.kp.ru/daily/26979/4038526/> (дата обращения: 03.10.2020).

2. Продаём под электронный ключ правительство, коммерсантов, квартиры [Электронный ресурс] // 47 news: Сетевое издание (сайт). URL: <https://47news.ru/articles/156549/> (дата обращения: 05.10.2020).

3. На московскую семью тайно зарегистрировали таксопарк и повесили долги [Электронный ресурс] // ВестиRU: Сетевое издание (сайт). URL: <https://www.vesti.ru/article/2478767> (дата обращения: 07.10.2020).

4. Хачатурова С. С. / Электронная цифровая подпись - удостоверение подлинности документа / С. С. Хачатурова. — Наука, техника и образование. 2016. №9 (27).

5. Власти проведут эксперимент с дистанционной выдачей электронной подписи [Электронный ресурс] // РБК: Сетевое издание (сайт). URL: https://www.rbc.ru/technology_and_media/18/10/2019/5da876a89a79472c0bcd51a3 (дата обращения: 07.10.2020).

6. Костенков В. С., Тимошенко Н.А. / Особенности проверки подлинности документов и их авторства в контексте научно-технологического развития Российской Федерации / В. С. Костенков, Н.А. Тимошенко // Актуальные эколого-политологические аспекты современности: сборник научных трудов II научно-практической конференции, 3 марта 2020 г. - Донецк: ГОУВПО «ДОННТУ», 2020. - Стр. 52 – 55.

7. Вершинская О. Н., Когаловский М. Р., Ершова Т. В. и др. / Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. — М.: Институт развития информационного общества, 2009. — 160 с. — ISBN 978-5-901907-20-7

8. Костенков В. С., Данилов В. В. / Особенности научно-технологического развития Российской Федерации в контексте проверки подлинности документов и их авторства / В. С. Костенков, В. В. Данилов // Вестник ДонНУ. Сер. Г: Технические науки. 2020. № 3 - Стр. 38 – 42.

Сведения об авторах

Костенков Владислав Сергеевич – аспирант кафедры радиофизики и инфокоммуникационных технологий; Донецкий национальный университет, Донецк; E-mail: vlad.kostenkov2016@yandex.ru

Данилов Владимир Васильевич - доктор технических наук, профессор, заведующий кафедрой радиофизики и инфокоммуникационных технологий, Донецкий национальный университет, Донецк; E-mail: ut5iv@mail.ru

Тимошенко Нина Александровна - кандидат юридических наук, доцент кафедры уголовного права и процесса, Донецкий национальный университет, Донецк; E-mail: n.timowenko@gmail.com

About the authors

Kostenkov Vladislav Sergeevich – postgraduate student of the Department of Radiophysics and Infocommunication Technologies; Donetsk National University, Donetsk; E-mail: vlad.kostenkov2016@yandex.ru.

Danilov Vladimir Vasilievich – Doctor of Technical Sciences, Professor, Head of the Department of Radiophysics and Infocommunication Technologies,

Donetsk National University, Donetsk; E-mail: ut5iv@mail.ru.

Tymoshenko Nina Aleksandrovna – Candidate of Legal Sciences, Associate Professor of the Department of Criminal Law and Procedure, Donetsk National University, Donetsk; E-mail: n.timowenko@gmail.com.