УДК 004.056.53:656.078

ВЕРИФИКАЦИЯ ПЕРВИЧНОЙ ТРАНСПОРТНОЙ ДОКУМЕНТАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ СВЯЗНЫХ СПИСКОВ

В. Д. Бойко
Одесский национальный политехнический университет

Аннотация. *В статье освещаются риски и проблемы, связанные с переходом на электронную форму первичной транспортной документации. Предлагается использование связных списков (блокчейн-технологии) в качестве средства защиты документооборота. В качестве доказательства работоспособности концепции был создан концептуальный прототип использования связных списков для документов стандарта OPEN-OASIS на базе языка python.*

Ключевые слова: *связные списки, блокчейн, хэш-суммы, транспорт, информационные системы, уязвимость, кибербезопасность, кибератака, информационная безопасность, криптография.*

Введение

Современный транспортный бизнес все больше переходит от бумажных носителей к электронным. Распространение различных конечных устройств ввода информации (планшетов, телефонов, терминалов, сканеров штрихкода, датчиков прямого съема данных) привело к тому, что все больший объем документации ведется напрямую в электронном виде, минуя бумажный носитель.

К первичной транспортной документации (ПТД) могут относиться различные виды документов в зависимости от транспортной системы и контекста ее использования.

Например, для автомобильного транспорта этот перечень включает в себя: путевой лист, который предназначен для учета транспортной работы (объемы перевезенных грузов и транспортной работы грузового автомобиля, выполнение расчетов между перевозчиком и заказчиком автомобильного транспорта и так далее) и товарно-транспортные накладные. При этом путевые листы содержат необходимые данные об объеме израсходованного горючего, что может использоваться не только для списания бензина, но и для расчета экосбора [1]. Для судоходства: судовой журнал, машинный журнал, санитарный журнал, журнал операций со сточными водами, журнал операций с мусором и так далее [2].

Ведение ПТД в электронной форме (ЭПТД) напрямую позволяет снизить накладные расходы и затраты на распечатку, на распознавание, на хранение документов. Кроме этого, ведение документации в электронной форме создает дополнительные выгоды: упрощается и улучшается интеграция в общую управляющую информационную сеть предприятия, не требуются затраты на переход от бумажной к электронной форме информации, увеличивается оперативность обработки информации.

Большинство систем ЭПТД структурно можно разделить на серверную и клиентскую части. Серверная часть находится в пределах вычислительного центра транспортного учреждения либо вынесена в облачную структуру и предназначена для выполнения сбора, хранения и анализа данных о работе транспортной системы. Как правило, к серверной части имеет доступ только определенная часть служащих компании (аналитики, системные администраторы, люди на руководящих должностях). Клиентская часть ЭПТД предназначена для эксплуатации непосредственно рядовым персоналом и является наименее защищенной от атак, направленных на фальсификацию данных в системе, поскольку большую часть времени находится вне поля зрения лиц, отвечающих за безопасность (в том числе кибернетическую и информационную) транспортной компании. Как правило, в таких системах фиксируется взаимодействие с внешними лицами, которые отслеживают процесс со своей стороны.

Наряду с перечисленными выше выгодами в виде упрощения и удешевления ведения документации переход к электронной форме первичной транспортной документации связан с дополнительными рисками.

Форма хранения информации в ЭПТД открывает возможности для злоупотребления — электронный носитель все еще остается гораздо более уязвимым для различного рода фальсификаций, чем бумажный, при этом выявление факта фальсификации сильно осложняется. Фальсификация документации (атака на систему ведения документации) может происходить различными способами: от прямой подмены содержимого документа в файловой системе или базе данных до взлома управляющего программного обеспе-

чения через выявленные или известные заранее уязвимости.

Целью статьи является анализ недостатков существующих систем защиты от фальсификации клиентской части ЭПТД. Предлагается использование связных списков (блокчейн-технологии) в качестве средства защиты документооборота.

1. Риски и безопасность ЭПТД

По данным международной службы по обеспечению безопасности в области киберугроз Symantec Security, каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд долл. США [3]. Несмотря на принимаемые меры законодательного и технологического характера, количество злоупотреблений в сфере кибербезопасности неуклонно растет.

Практика показывает, что в современных ЭПТД уделяется недостаточное внимание вопросам защиты от атак на систему с целью фальсификации документов, доступа к потенциально ценной для конкурентов информации и так далее. В большинстве случаев ЭПТД не защищена никак либо защищена слабо. Например, в обзорной работе [1] описываются системы, базирующиеся на пакете офисных приложений Microsoft Access/Office, которые защищены слабыми криптографическими системами или не защищены вообще.

Средства защиты, встроенные в ЭПТД в виде «замков» приложений, при условии, что данные внутри приложения не шифруются, являются заведомо недостаточными. Любое программное обеспечение потенциально подвержено взлому и атакам, поэтому данные, которые хранятся в открытой форме (например, в виде отдельных файлов или записей в базе данных) либо зашифрованы криптографически слабой системой (например, запароленным zip-архивом или парольной защитой документа Microsoft Office), будут рано или поздно скомпрометированы.

Таким образом, требуется надежная криптографическая система, которая бы позволила предотвратить фальсификацию данных ЭПТД даже при взломе клиентской части ЭПТД. Кроме того, в случае транспортных систем такого рода защита должна отвечать специфике отрасли — в частности, допускать эксплуатацию в условиях слабого развития информационной инфраструктуры и возможного отсутствия связи с центральным сервером предприятия либо в условиях экономической нецелесообразности организации такого доступа.

2. Существующие системы ЭПТД

Существует несколько общепринятых подходов к идее защиты данных в ЭПТД [4]. В частности, к ним относятся:

- защита данных в приложении с использованием сильной криптографической системы с симметричными ключами;
- защита данных в приложении с использованием сильной криптографической системы с ассиметричными ключами, с возможным участием заказчика;
- квитирование обмена данными.

Рассмотрим их подробнее.

2.1. Сильная криптографическая система с симметричными ключами

В этом случае в систему ЭПТД встраивается сильная криптографическая система (наиболее известной из них является симметричная и ассиметричная версии PGP/GnuPG). При этом даже если приложение будет взломано, злоумышленник не сможет получить доступ к данным, хранящимся в системе в зашифрованном виде. Однако если в случае обычных пользовательских систем криптографической защиты достаточно, то в случае ЭПТД возможны определенные сложности.

Как было сказано выше, сильная криптографическая система подразумевает использование для хранения данных системы симметричного или ассиметричного шифрования. При этом ЭПТД требует постоянного добавления данных в процессе работы транспорта. Например, в автотранспортной компании, занимающейся международными перевозками, транспортный лист обычно представляет собой документ, который выдается сразу на всю командировку — и заполняется в ее процессе. Поэтому у непосредственного пользователя системы сбора ЭПТД, как правило, имеется свой ключ для внесения данных в систему. Это делает систему уязвимой со стороны непосредственного пользователя: получив доступ к данным, он может использовать свой ключ для «открывания» системы и изменения информации. Кроме того, ключ может быть похищен или подменен непосредственно в момент использования, поскольку в процессе эксплуатации он находится в непосредственной близости от аппаратного средства ЭПТД.

2.2. Защита данных в приложении с использованием сильной криптографической системы с ассиметричными ключами, с возможным участием заказчика

Вариантом предыдущей системы является использование защиты ЭПТД с помощью технологии открытых ключей шифрования или ассиметричной криптосистемы. При таком подходе в системе существует открытый и закрытый ключ. Данные вносятся при помощи открытого ключа, а полный доступ к системе обеспечивается только с помощью закрытого ключа. При этом наличие только открытого ключа позволяет дополнять содержимое системы новыми записями, но не позволяет читать содержимое записей, внесенных в систему.

В такой системе непосредственный пользователь ЭПТД имеет на руках средство сбора информации и открытый ключ, а руководство и лица с доступом к базе данных имеют закрытый ключ. Такая система является наиболее предпочтительной для работы в ЭПТД, хотя и редко где внедрена.

Недостатком такой системы является возможность атак типа man-in-middle. Кроме того, система не обеспечивает возможности контроля общей целостности данных, поэтому без доступа к закрытому ключу может быть построена такая схема фальсификации, при которой данные, внесенные в базу в присутствии заказчика, могут быть позже удалены до того, как информация будет синхронизирована с центральной базой данных.

Вариантом использования криптографической системы является использование системы открытых ключей с вовлечением в процесс подписания документа заказчика. В этом случае документация шифруется либо дополнительно заверяется электронной цифровой подписью с ключом заказчика.

В целом такая система является вполне надежной, однако на практике возникает проблема плохой и неоднородной оснащенности заказчиков средствами как аппаратной, так и программной инфраструктуры. В частности, существуют сложности с распределением среди заказчиков открытых ключей и учетом авторства подписи открытым ключом: если такой учет не ведется и документ шифруется ключом без авторства, злоумышленник может добавить свое сообщение, получив доступ к любому из открытых ключей либо сгенерировав таковой самостоятельно.

Кроме того, следует учитывать существующую тенденцию к законодательному запрету сильной криптографии в некоторых странах.

2.3. Квитирование обмена данными

Еще один путь решения проблемы — внедрение системы квитирования транзакций через внешнюю систему связи. В каком-то смысле это информационный аналог бумажной системы двойной записи, когда транзакции внутри системы ЭПТД синхронно дублируются на центральном либо резервном сервере.

При такой системе каждое действие фиксируется отправлением полной или частичной «квитанции» о действии на сервер транспортной организации. Таким образом, ведется параллельно два журнала записей — внутри средства ЭПТД и на внешнем сервере. При этом, чтобы сэкономить на передаче данных, может использоваться частичная передача данных, при которой на сервер передается только контрольная сумма транзакции, а основная часть документа синхронизируется позже, со сверкой контрольных сумм клиентской и серверной частей.

При этом специфика эксплуатации транспортных средств состоит в том, что внешняя связь не всегда доступна и часто работает с перебоями, особенно в местах с недостаточным или затрудненным покрытием беспроводными системами связи. Кроме того, внешние каналы связи считаются уязвимыми (например, зафиксированы случаи организации ложных микросот мобильной связи и перехвата сетевого трафика), поэтому квитируемая система также имеет уязвимости и подвержена атакам.

3. Система защиты ЭПТД с использованием технологии связных списков

В данной работе предлагается система, основанная на использовании технологии связных списков (блокчейн-технологии, blockchain). Такая система получила широкую известность благодаря использованию для децентрализованного учета внутри систем так называемых цифровых валют (криптовалют). В частности, механизм блокчейна был впервые использован для обеспечения независимого, неадминистрируемого и децентрализованного учета системы криптовалют Bitcoin [5]. При этом область применения математического аппарата технологий связных списков имеет намного более широкое применение, в частности, в финансовом и банковском секторах, при выявлении мошенничества в различного рода реестрах и так далее.

Блокчейном называют связный список блоков информации, который представляет собой непрерывную последовательную цепочку данных. Каждое следующее звено цепочки верифицируется содержимым предыдущего звена и в

свою очередь служит основой для верификации следующего звена (см. рис. 1). При этом информация о транзакциях может храниться как в зашифрованном, так и в открытом виде (что снимает проблему в тех случаях, когда использование сильной криптографической системы запрещено законодательно). Для верификации записей используется контрольная сумма (хэш), при этом каждая следующая запись включает в себя хэш предыдущей записи, поэтому попытка заменить одно или несколько звеньев цепи, в частности, сфальсифицировать последовательность записей, приведет к разрушению связности системы. Это позволяет выявить факт фальсификации [6].

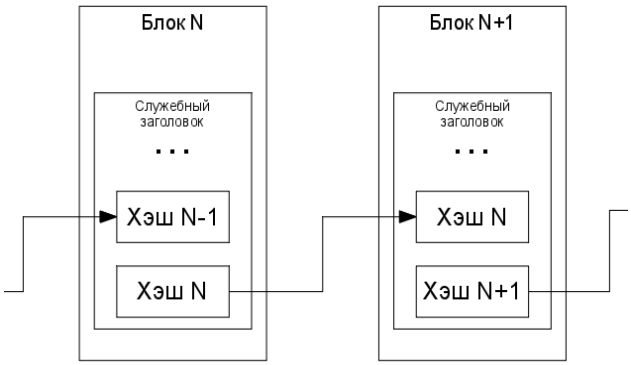

Рис. 1. Базовая структура работы технологии связных списков

Система ЭПТД, основанная на технологии связных списков, будет лишена указанных выше недостатков, она не будет требовать дорогостоящей и ненадежной системы квитирования по внешнему каналу связи, будет предъявлять минимальные требования к инфраструктуре заказчика. При этом система цепочек взаимосвязанных записей позволит верифицировать ПТД, выявляя факты несанкционированного вторжения и попыток изменения (фальсификации) данных, хранимых в системе.

Благодаря своей гибкости предлагаемая система может быть реализована на нескольких разных уровнях ведения записей и аудита. Такие уровни организационно могут быть реализованы в следующей форме:

- базовый уровень;
- продвинутый уровень;
- глобальный уровень.

На базовом уровне исходный ключ-звено остается у лица, ответственного за выдачу и регистрацию ПТД, и может изменяться ежедневно либо с началом рейса. Таким образом, начальное звено цепочки связных списков будет находиться у непосредственного руководителя подразделения и может использоваться для повседневной верификации ПТД либо для верификации ПТД на один рейс.

На продвинутом уровне основной ключ-звено принадлежит владельцу предприятия, а контроль осуществляется уже на уровне всего предприятия. Преимуществом такой системы является возможность контроля за документооборотом на уровне всего предприятия, а недостатком — «нестираемость» ведения архивных записей: при неверном вводе в систему информации исправить что-то возможно только до осуществления транзакции (т. е. до записи следующего звена с фиксирующей предыдущее хэш-суммой). Это может представлять проблему, особенно при обнаружении ошибок больших сроков давности.

Для глобального уровня контроль за ПТД осуществляется в течение всего времени эксплуатации системы и, после соответствующей сертификации, может служить в том числе подтверждающим документом для внешних проверяющих инстанций.

Общие алгоритмы работы схемы для клиентской (генерирующей) и серверной (верифицирующей) частей ЭПТД базового уровня приведены на рис. 2 и рис. 3.

В процессе работы клиентской части ЭПТД в начале происходит генерация исходного блока кода для лица, ответственного за выдачу документа. Затем для исходного блока вычисляется хэш-сумма, которая включается в тело документа. Таким образом, начальное звено связного списка остается у этого лица.

Далее по алгоритму происходит последовательное включение в документ новой информации. При этом на каждой итерации алгоритма происходит добавление к документу нового блока информации, добавление хэш-суммы из предыдущей итерации (это может быть реализовано как с помощью служебных полей документа, так и с помощью отдельной буферной переменной — поэтому в алгоритме вопрос работы с переменной вынесен в отдельные действия), кроме того, в документ добавляется хэш-сумма текущей итерации. Таким образом, создается непрерывная цепочка из связанных друг с другом блоков (рис. 1).

Алгоритм серверной части ЭПТД построен на обратной верификации связных списков, при этом работа по сверке хэш-сумм и блоков происходит в обратном порядке следующим образом.

Происходит инициализация буферной переменной. В момент инициализации буферная переменная имеет нулевое значение, далее в нее будут вноситься хэш-суммы из тела документа.

Далее в буферную переменную сохраняется последняя из добавленных в документ хэш-сумм, после чего эта хэш-сумма удаляется из тела документа. На следующем шаге алгоритма вычисляется проверочная хэш-сумма оставшегося тела документа. Затем выполняется сверка контрольной хэш-суммы с хэш-суммой, хранящейся в буферной переменной.

Рис. 2 Блок-схема работы клиентской части ЭПТД

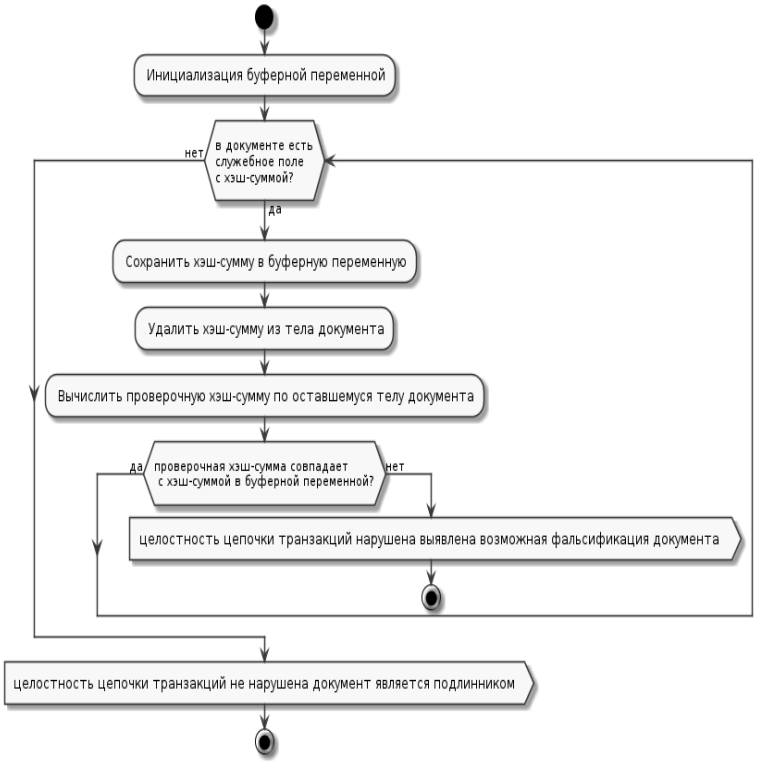

Рис. 3. Блок-схема работы серверной части ЭПТД

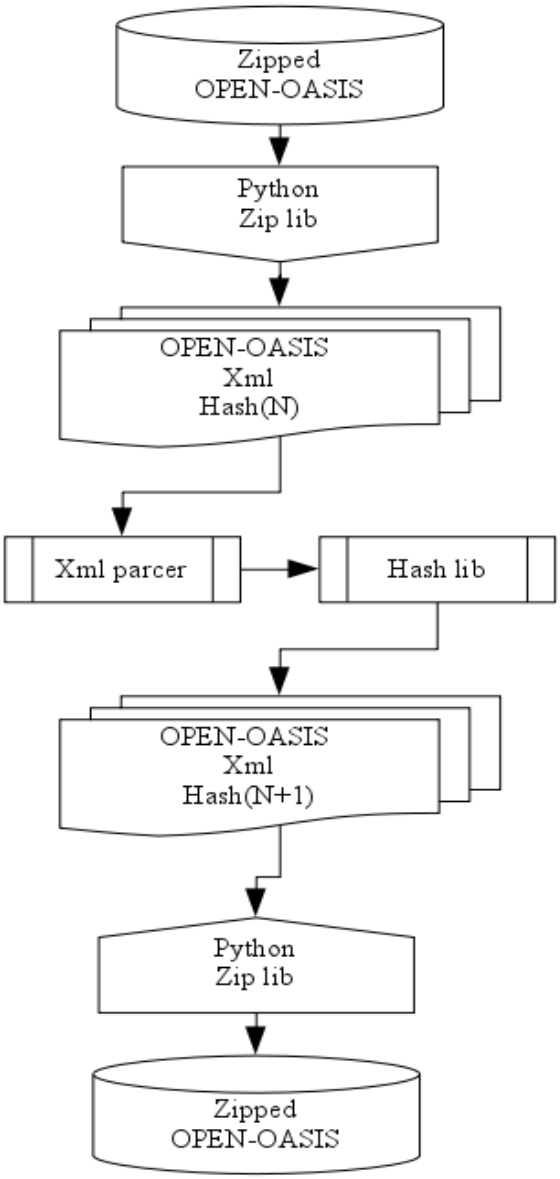

Рис. 4. Структурная схема обработки данных в клиентской части концептуального прототипа

Если суммы не равны, программа сообщает о нарушении целостности цепочки списков, что свидетельствует о возможной фальсификации документа.

Сравнение хэш-сумм последовательно выполняется до тех пор, пока не будет достигнуто последнее звено цепи блоков, то есть начальное звено цепи, которое находится у лица, ответственного за выдачу документа. Таким образом, если алгоритм достиг конца и при этом не было выявлено несовпадения хэш-сумм — целостность цепочки не нарушена, что будет свидетельствовать о том, что содержимое документа не было фальсифицировано.

Задействованная в алгоритме буферная переменная используется для хранения хэш-сумм в промежутке между добавлением новой информации в документ. В некоторых реализациях алгоритма блокчейна такая переменная включается непосредственно в текст документа, что заметно упрощает работу алгоритма. Однако такое решение приводит к засорению документа служебной информацией и увеличивает риск нарушения цепочки из-за непреднамеренного редактирования буферной переменной (ошибочное редактирование или удаление какой-то части переменной пользователем при добавлении информации в документ) либо приводит к усложнению прототипа из-за необходимости дополнительной защиты от случайного изменения хэш-суммы в тексте документа. Поэтому в концептуальном прототипе ЭПТД на стадии добавления информации в документ для хранения буферной переменной используется служебное поле документа, невидимое для пользователя при работе с документом в обычном режиме редактирования и таким образом защищенное от случайного изменения либо удаления. В прототипе, описаном ниже, для этих целей используется поле XML-документа META-INF/documentsignatures.xml, однако такая схема работы не является принципиальной и на следующих стадиях работы может быть изменена. На стадии верификации документа буферная переменная хранится отдельно от документа. Для упрощения архитектуры прототипа и увеличения общего быстродействия системы ЭПТД буферная переменная вынесена в переменную внутри кода программы верификации.

4. Концептуальный прототип системы защиты ЭПТД на основе технологии связных списков с использованием языка python

С целью доказательства верности концепции (Proof of Concept) был создан концептуальный прототип системы на языке python, включающий в себя серверную и клиентскую части.

В качестве основы хранения информации при концептуальном прототипировании был выбран формат OPEN-OASIS — открытый формат хранения документации, позволяющий работать со служебными полями внутри документа и поддерживающий средства работы с XML. Формат может быть использован в виде открытой части либо в виде запакованного zip-архиватором файла.

В качестве механизма хэширования использовалась библиотека hashlib, поставляемая в базовом дистрибутиве языка python. Данная библиотека может использовать следующие программные реализации алгоритмов хэширования: md5, sha1, sha224, sha256, sha384, sha512. Стандарт SHA-256 используется в криптовалюте Bitcoin и является оптимальным для приведен-

ной схемы [7]. Большинство перечисленных выше алгоритмов входит в семейство SHA-2, которое построено на основе использования структуры Меркла — Дамгора. Эта реализация все еще остается стандартом и вполне подходит для создания концептуального прототипа, однако на стадии создания MVP (minimum viable product — минимально жизнеспособного продукта) рекомендовано использование алгоритма SHA-3 (Keccak), который является более устойчивым к возникновению коллизий.

Для парсинга XML в прототипе используются библиотеки, поставляемые с языком python (xml.etree.ElementTree и библиотека zipfile). Создание MVP предполагает использование внешних инструментальных средств (библиотеки lxml, BeautifulSoup, Expat с библиотекой xml.parsers.expat). Кроме того, рассматривается возможность использования специализированной библиотеки работы с документами OpenOffice odfpy.

Для хранения данных в теле документа (в частности, при использовании буферной переменной) использовался внутренний файл документальной структуры META-INF/documentsignatures.xml, что соответствует стандарту OPEN-OASIS, однако в принципе возможно использование и других, в том числе скрытых от пользователя частей структуры документа. При работе с концептуальным прототипом было опробовано хеширование как определенной части документа, так и всей его структуры (т. е. с учетом добавления в схему XML дополнительных служебных частей).

Документ OpenDocument формата OPEN-OASIS (.odt, .odc) является zip-архивом, который содержит в себе файловую иерархию редактируемого документа — xml-документ, служебные xml-файлы, включая используемый в алгоритме documentsignatures.xml, и другие файлы.

Прототип структурно состоит из клиентской и серверной (контролирующей) частей. Процесс обработки данных в клиентской части продемонстрирован на рис. 4. Сжатый документ OPEN-OASIS с помощью встроенной библиотеки python распаковывается из zip-архива в набор файлов (в основном формата xml), далее выполняется обработка xml-файлов парсером (в том случае, если необходимо получить какие-либо служебные данные, например, предусмотрено хранение буферной переменной), после чего вычисляется хэш-сумма части файлов либо всего файлового набора целиком. Далее хэш-суммы добавляются в файлы документа, затем выполняется процесс упаковки документа, в результате чего получается файл для следующей итерации.

Серверная (контролирующая) часть также вначале осуществляет распаковку zip-архива в последовательность xml-файлов, после чего выполняет последовательную верификацию контрольных сумм, описанную в разделе 3, проверяя таким образом целостность цепочки изменений документа.

Полученный прототип уверенно определяет попытки фальсификации документов различного типа (фальсификация содержимого либо хэш-сумм), однако, как было замечено выше, при разработке MVP рекомендуется использование более совершенных инструментов, в частности, устойчивого к коллизиям семейства алгоритмов SHA-3 (Keccak).

5. Выводы

В статье рассмотрена проблема защиты от фальсификаций документооборота ЭПТД. Проведен анализ недостатков существующих систем защиты от фальсификации клиентской части ЭПТД с учетом использования их в транспортной отрасли. Предложено использование связных списков (блокчейн-технологии) в качестве средства защиты документооборота. Описана структура концептуального прототипа защиты документооборота ЭПТД от фальсификаций, выполненная на базе технологии связных списков.

Список использованной литературы

1. Романенкова, О. Н., Организация информационных потоков в управлении логистикой на автомобильном транспорте [Текст] //Экономика. Налоги. Право. – 2014. – №. 5.

2. Локтионов, А. Н., Иванен, Д. Г., Проблемы и особенности сбора информации для оценки судов [Текст] //Имущественные отношения в Российской Федерации. – 2011. – №. 3.

3. Карпова, Д. Н., Киберпреступность: глобальная проблема и ее решение [Текст] //Власть. – 2014. – №. 8.

4. Gragido, W. et al., Blackhatonomics: An Inside Look at the Economics of Cybercrime [Text] – Newnes, 2012.

5. Champagne, P., The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto [Text] //E53. – 2014.

6. Ammous, S., The Bitcoin Standard: The Decentralized Alternative to Central Banking. [Text] – John Wiley & Sons, 2018.

7. Antonopoulos, A. M., Mastering Bitcoin: Programming the open blockchain. [Text] – "O'Reilly Media, Inc.", 2017.

References

1. Romanenkova, O. N. (2014), "Organization of information flows in the management of logistics in road transport" [Organizacija informacionnyh potokov v upravlenii logistikoj na avtomobil'nom transporte], *Economy. Taxes. Law*, № 5.
2. Loktionov, A. N. and Ivanen, D. G. (2011), "Problems and features of the collection of information for the assessment of ships" [Problemy i osobennosti sbora informacii dlja ocenki sudov] *Property relations in the Russian Federation*, №3
3. Karpova, D. N. (2014), "Cybercrime: a global problem and its solution" [Kiberprestupnost': global'naja problema i ee reshenie], *Power*, № 8.
4. Gragido, W.; Molina, D.; Pirc, J. & Selby, N. (2012), *Blackhatonomics: An Inside Look at the Economics of Cybercrime*, Newnes.
5. Champagne, P. & Nakamoto, S. (2014), *The book of Satoshi : the collected writings of Bitcoin creator Satoshi Nakamoto*, e53 Publishing, LLC.
6. Ammous, S. (2018), *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley.
7. Antonopoulos, A. M. (2017), *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media.

VERIFICATION OF PRIMARY TRANSPORT DOCUMENTATION USING THE TECHNOLOGY OF LINKED LISTS

V. D. Boyko
Odessa National Polytechnic University

Abstract. *The paper highlighted risks and dangers associated with the transition to the electronic form of primary transport documentation and the related possibility of unauthorized changes to the information in the primary workflow. The analysis of the shortcomings of the existing systems of protection against falsification of the client part of the electronic form of primary transport documentation was carried out. The analysis examined various cryptography systems, including the system of queuing and systems of symmetric and asymmetric encryption. In connection with the specifics of the transport industry, implying poor mobile communications and an undeveloped customer infrastructure, the difficulties of introducing traditional workflow protection tools were shown. It was proposed using linked lists (blockchain technology) as a basic document protection. Due to its flexibility, the proposed system can be implemented at several different levels of record keeping and auditing. Information about transactions can be stored both in encrypted and in open form (which removes the problem in cases where the use of a strong cryptographic system is prohibited by law). The concept of using the blockchain system at a basic, advanced and global level was developed. In the latter case, it makes possible external control of the enterprise. As proof of the concept for using linked lists there was built conceptual prototype with use python programming language and its hash() standard library of hashing function. This prototype used linked lists technology for fraud detection inside of OPEN-OASIS format documents and may use hashing algorithms SHA-2 family like sha256, sha384 and sha512. However, for MVP it is recommended using more collision-resistant algorithms, such as SHA-3 (Keccak) family.*

Keywords: *linked lists, blockchain, hash sums, transport, information systems, vulnerability, cybersecurity, cyber-attack, information security, cryptography*

ВЕРИФІКАЦІЯ ПЕРВИННОЇ ТРАНСПОРТНОЇ ДОКУМЕНТАЦІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЗВ'ЯЗАНИХ СПИСКІВ

В. Д. Бойко
Одеський національний політехнічний університет

Анотація. *У статті висвітлюються ризики і проблеми, пов'язані з переходом на електронну форму первинної транспортної документації, та пов'язані з цим можливості несанкціонованої зміни інформації в первинному документообігу. Проведено аналіз недоліків існуючих систем захисту від фальсифікації клієнтської частини електронної форми первинної транспортної документації. Досліджено різні криптографічні системи, зокрема системи квітування та систем симетричного і аси-*

метричного шифрування. У зв'язку зі специфікою транспортної галузі, яка полягає у часто незадовільній якості мобільного зв'язку та нерозвиненій інфраструктурі клієнтів, описано проблеми застосування традиційних інструментів захисту робочих процесів. Пропонується використання зв'язаних списків (технологія блокчейн) у якості базової системи захисту документації. Завдяки своїй гнучкості пропонована система може бути реалізована на декількох різних рівнях ведення записів і аудиту. Було розроблено концепцію використання блокчейн-системи на базовому, розширеному та глобальному рівнях. В останньому випадку система може використовуватися для зовнішнього контроля підприємства. При цьому інформація про транзакції може зберігатися як в зашифрованому, так і у відкритому вигляді (що знімає проблему в тих випадках, коли використання сильної криптографічного системи заборонено на законодавчому рівні). Як доказ концепції використання зв'язаних списків було побудовано концептуальний прототип з використанням мови програмування Python та її стандартної бібліотеки функції гешування hash(). Цей прототип використовує технологію зв'язаних списків для виявлення фальсифікацій в документах формату OPEN-OASIS та може використовувати алгоритми гешування сімейства SHA-2, такі як sha256, sha384 і sha512. Однак для прототипу MVP-стадії рекомендується використання більш стійких до колізій алгоритмів, таких як сімейство SHA-3 (Keccak).

Ключові слова: *зв'язані списки, блокчейн, геш-суми, транспорт, інформаційні системи, вразливість, кібербезпека, кібератака, інформаційна безпека, криптографія.*

Получено 01.11.2018

Бойко Виктор Дмитриевич, кандидат технических наук, доцент Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина, E-mail: boyko-work@ukr.net, тел. +38-048-705-8584

Boyko Victor Dmitrievich, PhD, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: boyko-work@ukr.net, phone: +38-048-705-8584

ORCID ID: 0000-0001-5929-657X