Виктор С. Горбатов[1], Дмитрий А. Дятлов[2], Роман В. Наталичев[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: DADyatlov@mephi.ru, https://orcid.org/0000-0001-9967-6366
[3]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144

ОБ УСТОЙЧИВОСТИ ЛОГИСТИЧЕСКИХ СТРУКТУР НА ОСНОВЕ СМАРТ-КОНТРАКТОВ

DOI: http://dx.doi.org/10.26583/bit.2022.1.07

Аннотация. Одним из наиболее перспективных решений оптимизации логистических процессов является создание автоматизированных систем управления поставками на основе технологии распределенного реестра, в частности смарт-контракта. Однако кроме известных экономических преимуществ такой технологии целесообразность ее практического применения будет во многом определяться устойчивостью функционирования указанных систем управления в современных условиях угрозы дестабилизирующих воздействий. В настоящее время решение вопросов безопасности смарт-контрактов, как прикладных программ, сводится к проверке исходного кода приложений. Очевидно, что этого явно недостаточно для обеспечения надежности логистического управления, устойчивость которого может быть определена на основе известных методов оценки комплексной безопасности соответствующей ИТ-системы. Целью данного исследования является адаптация существующих методов аудита и оценки рисков информационной безопасности для ИТ-системы, использующей смарт-контракт, а предметом – обоснование применимости такого подхода к оценке защищенности логистических процессов с учетом особенностей смарт-контрактов. В работе рассмотрены особенности применения смарт-контрактов в логистических процессах, изложены соответствующие подходы к аудиту и оценке рисков функционирования системы логистического управления на основе смарт-контрактов. Разработаны рекомендации по практической реализации конкретных методик оценки защищенности ИТ-системы, использующей смарт-контракт, что ставится авторами в качестве цели дальнейшей работы. Результаты исследования могут быть полезны специалистам в области оптимизации логистических процессов и обеспечения информационной безопасности при разработке новых логистических схем на основе смарт-контрактов.

Ключевые слова: аудит, информационная безопасность, ИТ-системы, логистические процессы, оценка защищенности, оценка рисков, распределенный реестр, смарт-контракт, устойчивость.
Для цитирования: ГОРБАТОВ, Виктор С.; ДЯТЛОВ, Дмитрий А.; НАТАЛИЧЕВ, Роман В. ОБ УСТОЙЧИВОСТИ ЛОГИСТИЧЕСКИХ СТРУКТУР НА ОСНОВЕ СМАРТ-КОНТРАКТОВ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 70–81, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1403. DOI: http://dx.doi.org/10.26583/bit.2022.1.07.

Victor S. Gorbatov[1], Dmitriy A. Dyatlov[2], Roman V. Natalichev[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: DADyatlov@mephi.ru, https://orcid.org/0000-0001-9967-6366
[3]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144

On the sustainability of logistics structures based on smart contracts

DOI: http://dx.doi.org/10.26583/bit.2022.1.07

Abstract. One of the most promising solutions for optimizing logistics processes is the creation of automated supply management systems based on distributed registry technology, in particular a smart contract. However, in addition to the well-known economic advantages of such a technology, the expediency of its practical application will largely be determined by the stability of the functioning of these

control systems in modern conditions of the threat of destabilizing influences. Currently, the solution to the security issues of smart contracts as programs are reduced to checking the source code of applications. Obviously, this is clearly not enough to ensure the reliability of logistics management, the stability of which can be determined on the basis of known methods for assessing the complex security of the corresponding IT system. This study adapts existing methods for auditing and assessing information security risks for an IT system using a smart contract, and the subject is to substantiate the applicability of such an approach to assessing the security of logistics processes, considering the features of smart contracts. The paper considers the features of the use of smart contracts in logistics processes, outlines appropriate approaches to audit and risk assessment of the functioning of the logistics management system based on smart contracts. Recommendations have been developed for the practical implementation of specific methods for assessing the security of an IT system using a smart contract, which is set by the authors as the goal of further work. The results of the study can be useful to specialists in the field of optimization of logistics processes and information security when developing new logistics schemes based on smart contracts.

Keywords: audit, information security, IT systems, logistics processes, security assessment, risk assessment, distributed ledger, smart contract, sustainability.

For citation: GORBATOV, Victor S.; DYATLOV, Dmitriy A.; NATALICHEV, Roman V. On the sustainability of logistics structures based on smart contracts. IT Security (Russia), [S.l.], v. 29, n. 1, p. 70–81, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1403. DOI: http://dx.doi.org/10.26583/bit.2022.1.07.

Введение

Развитие информационных технологий продолжает менять модель отношений не только в социальной, но и в профессиональной сферах, все больше переводя существующие процессы взаимодействия в виртуальную информационную среду. Наблюдается изменение средств и способов коммуникации, например, вследствие глобализации торговых отношений, что в свою очередь, ведет к изменению принципов взаимодействия между различными организациями, участвующими в логистических процессах. Появляется необходимость в квалифицированных сотрудниках логистических компаний вследствие применения новых технологических логистических решений, таких, например, как автоматизированные системы управления, электронная идентификация товаров и спутниковое слежение за движением транспортных потоков. Глобализация торговых отношений требует оптимизации существующих форм рыночных коммуникаций, что выражается в отчетливой тенденции к снижению издержек на логистические операции. В основном – это максимальное сокращение жизненного цикла процесса по перемещению готовой продукции или сырьевых товаров благодаря реорганизации цепей поставок, оптимизации транспорта, новых технологий, автоматизации складских работ и централизации доставки [1].

Однако множество причин препятствуют успешному преобразованию цепей поставок [2], характерных для большинства логистических структур:

– недостаточная проработка маршрутов поставок;

– простой на промежуточных узлах цепочек поставок;

– обеспечение безопасности, в том числе информационной, перемещения ценных грузов;

– несовершенство законодательной базы.

В последнее время снижение устойчивости логистических операций к воздействию дестабилизирующих факторов характеризуется таким кризисным явлением в мировой экономики как недостаток товаров даже в экономически развитых странах (США, Великобритании и др.), что явилось следствием произошедшей в 2020 г. пандемии коронавирусной инфекции, вскрывшей новые проблемы в мировой (глобальной) логистике [3]. В первую очередь – это отсутствие «антикризисного плана» в создавшейся обстановке всеобщей изоляции, и как следствие, снижение объема мировых логистических операций.

Основными дестабилизирующими факторами такого кризиса можно назвать недостаточно быструю переориентацию с одного вида транспортировки на другой, слабое внедрение и применение новейших информационных технологий, неготовность перевода сотрудников логистических компаний на удаленную работу с сохранением эффективности осуществляемых бизнес-процессов. Иными словами, основной фактор – неготовность существующей системы управления к новым вызовам.

В качестве конкретных примеров необходимости изменений в мире логистики можно привести аварию контейнеровоза «Эвер Гивен» с блокировкой Суэцкого канала и убытком для мировой логистики в 9,6 млрд долл./день [4], а также кибератаку на трубопроводную систему в США Colonial Pipeline в мае 2021 г. В результате кибератаки остановилась работа трубопровода [5], для возобновления функционирования которого компания заплатила злоумышленникам около 4,4 млн долл. В последнем случае сказалось недостаточно полное понимание проблем обеспечения информационной безопасности (ИБ) и, как следствие, низкая оперативность и реагирование на произошедший инцидент.

Тенденцией последних нескольких лет по совершенствованию управления и повышению устойчивости логистических структур стало все более широкое использование таких приложений как смарт-контракты, встроенные в распределенный реестр (РР) и систематизирующие эффективное взаимодействие между большим количеством пользователей при недостаточном или полном отсутствии доверия между ними [6]. Известными экономическими преимуществами смарт-контрактов являются более легкий и быстрый доступ к логистическим услугам и существующей инфраструктуре для обеспечения запасного транспортного канала [7], а также снижение количества сопроводительных документов, уменьшение дополнительных расходов для разрешения возникающих инцидентов, устранение операционных ошибок.

Постановка задачи и методология оценки рисков использования технологии РР как некоторой обобщенной ИТ-системы приведены в [8]. В настоящей работе эти вопросы рассмотрены применительно к такому приложению как смарт-контракт с учетом его особенностей.

1. Смарт-контракт как инструментарий повышения эффективности логистики

Идея смарт-контракта была предложена американским ученым Ником Сабо в 90-х годах прошлого века [9]. По сути, смарт-контракт – это компьютерная программа с заранее определенными протоколами, встраиваемая в оборудование или программное обеспечение для выполнения различных договорных условий. Система РР предоставляет среду коммуникаций, в которую можно поместить смарт-контракт для его непосредственной реализации.

Смарт-контракт автоматизирует проводимые транзакции по определенным правилам, например, действия могут выполняться строго при наступлении заданных событий, и выполнение данного алгоритма не может быть отменено, остановлено или заменено. В этом случае размещение в системе РР обеспечивает смарт-контракту взаимодействие с управляющей (выполнено условие или нет) и исполняющей (действие выполняется или нет) информацией. Жизненный цикл смарт-контракта[1] представлен на рис. 1.

[1]ISO/TR 23455:2019. Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems.

Рис. 1. Жизненный цикл смарт-контракта
Fig. 1. The life cycle of a smart contract

Прежде, чем создать контракт, необходимо договориться о его условиях: какие события ведут к каким действиям. Следующий шаг – создание самого смарт-контракта, то есть разработка алгоритма последовательности выполнения условий сделки и написание непосредственно программы. После этого смарт-контракт размещается в системе РР, чтобы все участники сделки видели и могли отслеживать прохождение этапов договора в рамках своих прав и компетенций. Затем смарт-контракт, как элемент системы РР, соединяется с внутренними и внешними источниками для получения и передачи данных для выполнения условий сделки. Когда все сформировано, смарт-контракт остается в положении ожидания внешнего события, прописанного в его алгоритме, и проверяет выполнение требований заключенной сделки. После наступления ожидаемого события происходит исполнение определенного действия смарт-контракта. До этого момента никаких действий в рамках смарт-контракта не происходит. Любые произошедшие изменения в системе записываются в реестр, реестр обновляется, и все участники системы видят, что происходит в реальном времени. Данные нельзя заменить, изменить, нельзя отказаться от совершенных действий, то есть обеспечиваются основные принципы ИБ – целостность и доступность используемых данных при обеспечении неотказуемости от совершенных действий. Еще один принцип ИБ – конфиденциальность соблюдается ввиду того, что каждый из участников системы обладает только информацией в рамках своих прав и своей компетенции. Остальная информация скрыта в «глубинах» смарт-контракта.

Для чего же все это надо? Сотни лет логистическая система работает по проверенным временем законам и принципам. Что дает данное новшество? Есть ли в этом какая-либо выгода или польза? Стоит ли усложнять «новомодными штучками» отработанный алгоритм действий. Рассмотрим это на примере поставки груза, рис. 2.

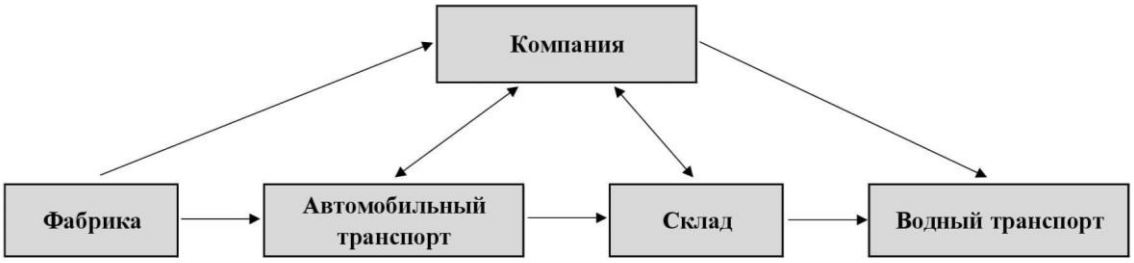

Рис. 2. Традиционная схема поставки груза
Fig. 2. Traditional cargo delivery scheme

Компания поставляет продукцию с фабрики двумя видами транспорта через промежуточный склад. При традиционной схеме поставки для прохождения этого процесса потребуется выполнение следующих операций:

1) отгрузка груза с фабрики на склад автомобильным транспортом;
2) сообщение с фабрики в компанию об отгрузке груза на склад;
3) сообщение из компании на склад об отгрузке в их адрес груза;
4) доставка груза на склад автомобильным транспортом;
5) сообщение со склада в компанию о доставке груза;
6) сообщение от автоперевозчика в компанию о доставке груза и счет за доставку;
7) оплата компанией доставки груза автоперевозчику;
8) заказ компании водного транспорта для отправки груза со склада;
9) отгрузка груза со склада для транспортировки водным транспортом;
10) сообщение со склада в компанию об отгрузке груза.

Такой же процесс по доставке груза с использованием смарт-контракта представлен на рис. 3.

Рис. 3. Схема поставки груза с использованием смарт-контракта
Fig. 3. Cargo delivery scheme using a smart contract

Для этой схемы поставки потребуется выполнение следующих информационных операций:

1) сообщение об отгрузке груза с фабрики записывается в смарт-контракт и автоматически передается в компанию и на склад;
2) сообщение о доставке груза на склад записывается в смарт-контракт и автоматически передается в компанию;
3) команда в компанию на оплату и оплата доставки груза автоперевозчику (выполняется смарт-контрактом автоматически);
4) заказ водного транспорта для отправки груза со склада (выполняется смарт-контрактом автоматически);
5) сообщение об отгрузке груза со склада записывается в смарт-контракт и автоматически передается в компанию.

Таким образом, при использовании смарт-контракта значительно сокращается количество ручных операций и время прохождения всех информационных процессов, в то время как в практике традиционных поставок для проведения подобных операций требуется время от нескольких часов до нескольких дней или даже недель. Нельзя забывать о том, что информационные процессы проходят через операторов, и чем больше участников

вовлечены в бизнес-операцию, тем большее количество людей в ней задействовано вместе с их оборудованием и сетями связи. Количество операторов при традиционной схеме гораздо больше, чем при использовании смарт-контракта. То есть снижается вероятность ошибок или утечки информации, а также возможность сговора отдельных участников между собой. Повышается «прозрачность» проводимой сделки и доверие между сторонами, участвующими в бизнес-операции.

Создание смарт-контракта исключает наличие иерархического управления, все участники контракта обладают равными правами, а операции выполняются по строго определенному алгоритму, то есть условия выполнения контракта не могут быть изменены в процессе его выполнения. Отсутствует возможность «давления» со стороны более сильного участника контракта на других участников, либо отказа от выполнения своих обязательств. Кроме этого, при несоблюдении условий контракта, штрафы и неустойки взыскиваются автоматически.

Размещение смарт-контракта в РР, то есть слияние двух самостоятельных технологий, создает систему смарт-контракта. Такая система отличается от первоначального замысла смарт-контракта [9] – набора обещаний, заданного в цифровой форме, для выполнения других обещаний, так как объединение с РР создает новое поколение независимых смарт-контрактов1. Такие системы имеют многоуровневую архитектуру [10], что требует соответствующих подходов и методов оценки их защищенности. В настоящее время нет общепринятой стандартной архитектуры РР с, размещенным в нем смарт-контрактом, поэтому в целях данной работы в основу исследования принята четырехуровневая модель архитектуры системы РР [8], представленная в табл. 1.

Таблица 1. Четырехуровневая модель архитектуры системы смарт-контракта

Уровень системы смарт-контракта	Уровень OSI	Технологические компоненты
Прикладной	Прикладной	Создание Интеграция Функционирование Приложения безопасности
Представления	Представления	Архитектура ПО, язык программирования Способы стимулирования Цифровые активы Функциональность Исполнение смарт-контрактов Управление правами доступа Способы увеличения пропускной способности
Транспортный	Сеансовый Транспортный	Консенсус Безопасность и приватность Исполнение транзакций
Физический	Сетевой Канальный Физический	Телекоммуникационные сети Телекоммуникационное оборудование Вычислительные системы

2. Постановка задачи исследования – оценка защищенности системы смарт-контракта

В настоящее время исследование смарт-контрактов проводится, в основном, на прикладном уровне и направлено на проверку исходного кода программ. Приложения

тестируются специалистами по ИБ, используя типовые подходы оценки надежности компьютерных программ, например, тестирование, проверка исходного кода и методология проектирования по контракту [11]. Но этих методов явно недостаточно при встраивании смарт-контрактов в систему РР, существующей и работающей в режиме реального времени, то есть при постоянном внесении изменений, в том числе в последовательность проводимых операций. И какой бы ни был объем тест-кейсов, он не в состоянии обеспечить достаточную проверку программного обеспечения. Следовательно, тестирование на прикладном уровне не может использоваться в качестве основного метода контроля защищенности системы смарт-контракта.

При функционировании смарт-контракта в РР блоки данных часто многократно обрабатываются различными узлами системы, то есть к уровню приложений относятся не только смарт-контракты. Также на этом уровне находятся программы, обеспечивающие взаимодействие между узлами РР, влияющие на:

- работу смарт-контракта,
- обмен данными и цифровыми активами,
- программы наблюдения за загрузкой данных и состоянием системы,
- программы отслеживания проводимых операций,
- программы защиты сети, резервного копирования и восстановления системы.

В этих программах и на других уровнях архитектуры системы также могут возникнуть уязвимости.

Таким образом, известные в настоящее время методы, применяемые для обеспечения ИБ смарт-контрактов, не учитывают в полной мере особенности архитектуры встраивания этих приложений в системы и сети бизнес-процессов. Требуется более детальный и всеобъемлющий подход к обеспечению безопасности таких систем, позволяющий определить потребности в защите информации и создании эффективной системы управления. Необходимо обеспечить своевременное реагирование на возникающие инциденты ИБ и применение технических, организационных, программных, правовых и других защитных мер для минимизации вероятности возникновения инцидентов.

Практическая реализация смарт-контрактов и перспективы их дальнейшего развития зависят от соблюдения основных принципов обеспечения ИБ, таких как аутентификация и обеспечение неотказуемости для участников сети, обеспечение надежности системы криптографическими ключами. Данные принципы либо игнорируются, либо им придается недостаточное значение, что приводит к отсутствию доверия и признанию их пока ненадежными системами, подверженными колоссальному риску [12].

Еще одним «слабым» звеном ИБ системы РР с размещенным в нем смарт-контрактом является обеспечение конфиденциальности, в частности данных проводимых транзакций, которые записываются в реестр. В этом направлении ведутся активные научные и практические работы, изучающие различные инструменты обеспечения конфиденциальности проводимых операций в системах РР, например: «Криптографические перемешивающие сети», «Кольцевая подпись», «Гомоморфное шифрование», «Доказательства с нулевым разглашением» [13]. Но, на данный момент, ни один из существующих методов не решает удовлетворительно эту проблему в целом, относительно производительности и объема данных, которые создаются участниками сети в процессе проведения транзакций [13].

Для решения проблем унификации технологии РР в 2016 г. был образован специализированный технический комитет ISO/TC 307 «Технологии блокчейна и распределенного реестра». Этот комитет ведет работу над десятью стандартами данных

технологий [14]. На сегодняшний день только четыре стандарта опубликованы, причем три из них в 2020 г. Первый стандарт ISO 23455 «Обзор и взаимодействие между смарт-контрактами в системах технологии блокчейна и технологий распределенного реестра» был опубликован в сентябре 2019 г., на основании которого и проходит проверка ИБ в отношении смарт-контрактов.

Для успешного интегрирования смарт-контракта, представляющего в совокупности с технологией PP ИТ-систему, в логистические процессы необходимо реализовать комплексный подход к обеспечению ИБ, определяющей устойчивость логистики на протяжении всего жизненного цикла существования системы – от планирования до эксплуатации и сопровождения. Иными словами, необходима организация систематического процесса, оценивающего все составляющие логистической системы, обеспечивающий безопасность проводимых операций и осуществляющий управление ИБ.

3. Методология оценки защищенности системы смарт-контракта

Наиболее полно решению поставленной выше задачи отвечает известная методология [15], предусматривающая совокупность организационных процедур, условно разделенных на три этапа:

- подготовительный,
- основной,
- заключительный.

Практическую реализацию указанных процедур можно проводить в рамках аудита ИБ, который наиболее полно отвечает требованиям по оценке защищенности информационных систем управления. По результатам аудита ИБ осуществляется принятие и выполнение решений по ИБ на всех этапах жизненного цикла, выявляются возможные уязвимости, повышается эффективность использования имеющихся технологических ресурсов.

Важнейшим элементом аудита, часто выделяемым в отдельную задачу, является совокупность процедур оценки рисков. Такая оценка позволяет определить ценность используемых данных и других активов системы, связанные с ними уязвимости и угрозы устойчивости системы, расставить их в приоритетном порядке с целью более эффективного распределения технологических ресурсов. Методология оценки рисков ИБ ИТ-систем в настоящее время хорошо изучена, достаточно унифицирована, имеет обширный опыт применения [16], что позволяет рассматривать ее в качестве основы для дальнейшей адаптации в целях оценки защищенности системы смарт-контракта.

Обобщенный процесс проведения оценки рисков и дальнейших мероприятий по их управлению применительно к системе смарт-контракта, в соответствии с [16–17], представлен на рис. 4.

Рис. 4. Оценка рисков ИБ системы смарт-контракта
Fig. 4. Risk assessment of the information security of the smart contract system

В зависимости от принятых в конкретной логистической структуре управленческих взаимодействий процедуры оценки рисков могут значительно различаться по методам, требованиям и масштабу, но основной их целью остается выявление рисков для активов структуры, а также их количественная и качественная оценки. Количественный и качественный метод – два основных подхода к оценке рисков ИБ [17], применяемые независимо друг от друга или одновременно, наиболее полно представлены в стандарте, использованном в [8] для системы РР. По аналогии для системы смарт-контракта можно рекомендовать к использованию те же методы оценки рисков:

1) «Анализ дерева отказов (FTA)»,
2) «Анализ надежности человека (HRA)»,
3) «Изучение опасности и работоспособности (HAZOP)»,
4) «Методы нечеткой логики»,
5) «Техническое обслуживание на основе надежности (RCM)».

В [8] также предложена алгоритмическая основа, которую можно использовать для практической реализации типовой методики оценки рисков системы смарт-контракта на базе «хорошей практики», предлагающей известный итеративный подход к проведению оценки рисков. Итоговый алгоритм применительно к системе смарт-контракта представлен на рис. 5.

Рис. 5. Алгоритм оценки рисков ИБ системы смарт-контракта
Fig. 5. Algorithm for assessing the risks of information security of the smart contract system

Приведенные выше методы не покрывают полностью процесс проведения оценки рисков ИБ и рекомендуются только как основа для адаптации существующих и создания новых технологий оценки рисков системы смарт-контракта. Необходимы комплексные мероприятия, сочетающие применение нескольких методов и технологий оценки рисков ИБ одновременно на соответствующих этапах проведения проверки. То есть разработка конкретной методики не должна строго ограничиваться методами, определенными в данной работе, и в дальнейшем допускается совместное использование с другими технологиями.

Также важным элементом методики является этап документирования всех результатов оценки защищенности системы смарт-контракта, на основе которого создается политика безопасности системы и составляется план управления рисками ИБ.

Заключение

Существующая тенденция по совершенствованию управления и повышению устойчивости логистических структур актуализирует все более широкое использование таких приложений, как смарт-контракты, встроенные в систему распределенного реестра. Смарт-контракты систематизируют эффективное взаимодействие между пользователями при недостаточном или полном отсутствии доверия между ними.

В то же время, их практическое внедрение во многом сдерживается из-за нерешенности многих вопросов обеспечения ИБ не столько на прикладном, сколько на системном уровне. Представленные в работе подходы по решению поставленной задачи создают методологическую основу для дальнейшего развития исследований в направлении разработки типовых методик оценки защищенности системы смарт-контракта с использованием хорошо зарекомендовавших себя методов аудита и управления рисками ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Белякова А.В. Значение логистики в условиях глобализации международного товародвижения. E-SCIO. 2020, № 4 (43), с. 597–607. URL: https://elibrary.ru/item.asp?id=42818426 (дата обращения 17.01.2022).
2. Захарова А.И. Основные проблемы транспортной логистики в России. Аллея науки. 2020, т. 2, № 4 (43), с. 7–10. URL: https://elibrary.ru/item.asp?id=42951263 (дата обращения 17.01.2022).
3. Воронецкий Д.А. Логистические тренды 2020–2021 года: жизнь во время и после пандемии. The scientific heritage. 2021, № 75–4 (75), с. 23–29. DOI: https://doi.org/10.24412/9215-0365-2021-75-4-23-29.
4. Калинина А.А. Особенности морских перевозок на примере Суэцкого канала. Известия института систем управления СГЭУ. 2021, № 1 (23), с. 123–125. URL: https://www.elibrary.ru/item.asp?id=45849004 (дата обращения 17.01.2022).
5. Демидов А. Глава Colonial Pipeline рассказал, сколько компания заплатила хакерам. Газета.ru. 19.05.2021. URL: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (дата обращения 17.01.2022).
6. Дмитриев А.В. Развитие технологии блокчейн в транспортно-логистических системах. Логистика – евразийский мост. Материалы XIV Международной научно-практической конференции. Красноярск, 24–29 апреля 2019. С. 98–103. URL: https://www.elibrary.ru/item.asp?id=37383916 (дата обращения 17.01.2022).
7. Irannezhad E. Is blockchain a solution for logistics and freight transportation problems? Transportation Research Procedia. 2020, vol. 48, p. 290–306. DOI: https://doi.org/10.1016/j.trpro.2020.08.023.
8. Durakovskiy A.P., Gorbatov V.S., Melnikov D.A., Dyatlov D.A. Security risk management methodology for distributed ledger systems. Conference: BICA*AI 2021: BICA Workshop at ACM IVA 2021, a virtual event. Fukuchiyama, Kyoto, Japan, September 14, 2021. SCI 1032, p. 1–17. DOI: https://doi.org/10.1007/978-3-030-96993-6_9.
9. Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. 1996. URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (дата обращения 17.01.2022).
10. Запечников Сергей В. Системы распределенного реестра как инструмент обеспечения доверия между участниками бизнес-процессов. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 37–53. 2019. DOI: http://dx.doi.org/10.26583/bit.2019.4.03.
11. Меркин Л.А., Резин Р.М., Васильев Н.К. Архитектура формально-верифицированной системы распределенного реестра InnoChain. Моделирование и анализ информационных систем. 2020, т. 27, № 4, с. 472–487. DOI: https://doi.org/10.18255/1818-1015-2020-4-472-487.
12. Будзко Владимир И., Мельников Дмитрий А. Исторический ракурс технологии «Blockchain». «Всё новое – хорошо забытое старое». Безопасность информационных технологий, [S.l.], т. 25, № 4, с. 23–33, 2018. DOI: http://dx.doi.org/10.26583/bit.2018.4.02.
13. Запечников Сергей В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций. Безопасность информационных технологий, [S.l.], т. 27, № 4, с. 108–123, 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09.
14. Будзко Владимир И., Милославская Наталья Г. Вопросы практического применения технологий блокчейна. Безопасность информационных технологий, [S.l.], т. 26, № 1, с. 36–45, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.1.04.
15. Макаренко С. И. Аудит ИБ: основные этапы, концептуальные основы, классификация мероприятий. Системы управления, связи и безопасности. 2018, № 1, с. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения 17.01.2022).
16. Кривякин К.С., Изотова А. Р., Федоров В. М. Методический подход к оценке рисков информационной безопасности предприятия. Экономинфо. 2018, т. 15, № 2, с. 82–90. URL: https://elibrary.ru/item.asp?id=35177684 (дата обращения 17.01.2022).
17. Склярук В.Л., Сергеева О.О. Методы оценки рисков информационной безопасности. Современные проблемы радиоэлектроники и телекоммуникаций. 2018, № 1, с. 219. URL: https://elibrary.ru/item.asp?id=38500295 (дата обращения 17.01.2022).

REFERENCES:

[1] Belyakova A.V. The significance of logistics in the context of globalization of international commodity circulation. E-SCIO. 2020, no. 4 (43), p. 597–607. URL: https://elibrary.ru/item.asp?id=42818426 (accessed: 17.01.2022) (in Russian).
[2] Zakharova A.I. The main problems of transport logistics in Russia. Alley science. 2020, vol. 2, no. 4 (43), p. 7–10. URL: https://elibrary.ru/item.asp?id=42951263 (accessed: 17.01.2022) (in Russian).
[3] Voronetskiy D.A. Logistics trends of 2020-2021: life during and after the pandemic. The scientific heritage. 2021, no. 75–4 (75), p. 23–29. DOI: https://doi.org/10.24412/9215-0365-2021-75-4-23-29 (in Russian).

[4] Kalinina A.A. Features of shipping on the example of the suez canal. News of the Institute of Control Systems SSUE. 2021, no. 1 (23), p. 123–125. URL: https://www.elibrary.ru/item.asp?id=45849004 (accessed: 17.01.2022) (in Russian).
[5] Demidov A. The head of Colonial Pipeline told how much the company paid hackers. Gazeta.ru. 19.05.2021. URL: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (accessed: 17.01.2022) (in Russian).
[6] Dmitriev A.V. Development of blockchain technology in transport and logistics systems. Logistics – Eurasian bridge. Materials of the XIV International Scientific and Practical Conference. Krasnoyarsk, 24–29 April 2019. P. 98–103. URL: https://www.elibrary.ru/item.asp?id=37383916 (accessed: 17.01.2022) (in Russian).
[7] Irannezhad E. Is blockchain a solution for logistics and freight transportation problems? Transportation Research Procedia. 2020, vol. 48, p. 290–306. DOI: https://doi.org/10.1016/j.trpro.2020.08.023.
[8] Durakovskiy A.P., Gorbatov V. S., Melnikov D.A., Dyatlov D.A. Security risk management methodology for distributed ledger systems. Conference: BICA*AI 2021: BICA Workshop at ACM IVA 2021, a virtual event. Fukuchiyama, Kyoto, Japan, September 14, 2021. SCI 1032, p. 1–17. DOI: https://doi.org/10.1007/978-3-030-96993-6_9.
[9] Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. 1996. URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed: 17.01.2022)
[10] Zapechnikov Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security, [S.l.], vol. 26, no. 4, p. 37–53, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.4.03 (in Russian).
[11] Merkin-Janson L.A., Rezin R.M., Vasilyev N.K. Architecture of the Formally-Verified Distributed Ledger System InnoChain. Modeling and Analysis of Information Systems. 2020, vol. 27, no. 4, 472–487. DOI: https://doi.org/10.18255/1818-1015-2020-4-472-487.
[12] Budzko Vladimir I., Melnikov Dmitry A. The historical view of the blockchain technology. The more things change, the more they stay the same. IT Security, [S.l.], vol. 25, no. 4, p. 23–33, 2018. DOI: http://dx.doi.org/10.26583/bit.2018.4.02 (in Russian).
[13] Zapechnikov Sergey V. The distributed ledgers ensuring privacy-preserving transactions. IT Security, [S.l.], vol. 27, no. 4, p. 108–123, 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09 (in Russian).
[14] Budzko Vladimir I., Miloslavskaya Natalia G. Issues of practical application of blockchain technology. IT Security, [S.l.], vol. 26, no. 1, p. 36–45, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.1.04 (in Russian).
[15] Makarenko S.I. Audit of information security - the main stages, conceptual framework, classification of types. Systems of control, communication and security. 2018, no. 1, p. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (accessed: 17.01.2022) (in Russian).
[16] Krivyakin K.S., Izotova A.R., Fedorov V.M. Methodological approach to risk assessment the enterprise information security. Economінfo. 2018, vol. 15, no. 2, p. 82–90. URL: https://elibrary.ru/item.asp?id=35177684 (accessed: 17.01.2022) (in Russian).
[17] Sergeeva O.O., Sklyaruk V.L. Methods of estimation of information security risk. Modern problems of radio electronics and telecommunications. 2018, no. 1, p. 219. URL: https://elibrary.ru/item.asp?id=38500295 (accessed: 17.01.2022) (in Russian).

Поступила в редакцию – 21 января 2022 г. Окончательный вариант – 15 февраля 2022 г.
Received – January 21, 2022. The final version – February 15, 2022.