НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2024 Том 24 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2024 Vol. 24 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

COMPUTER SCIENCE

doi: 10.17586/2226-1494-2024-24-6-949-961
УДК 004.056

Модель обеспечения непрерывности безопасного функционирования системы прослеживаемости качества продукции в условиях неустойчивой коммуникации

Ван Хиеу Лэ[1], Игорь Иванович Комаров[2]✉, Александр Андреевич Привалов[3], Антон Александрович Пыркин[4]

[1,2,4] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[3] Российский университет транспорта, Москва, 127994, Российская Федерация

[1] dragon220294@gmail.com, https://orcid.org/0000-0002-9413-5138
[2] i_krov@mail.ru✉, https://orcid.org/0000-0002-6542-4950
[3] privalov1985@ya.ru, https://orcid.org/0000-0001-8977-152X
[4] a.pyrkin@gmail.com, https://orcid.org/0000-0001-8806-4057

Аннотация

Введение. Технологии доказательного подтверждения качества продукции оказывают положительное влияние на широкий спектр социальных и экономических процессов. Одна из проблем реализации таких технологий определяется противоречием между необходимостью обеспечения открытого доступа к информации об этапах технологического процесса и конфиденциальностью части данных. Применение строгих криптографических процедур для разрешения данного противоречия часто невозможно из-за наличия ресурсных ограничений, в частности — отсутствия непрерывной телекоммуникации между причастными сторонами. Полученные результаты направлены на обеспечение реализуемости систем прослеживаемости качества продукции в условиях ресурсных ограничений. Они базируются на новом архитектурном решении и комплексировании классических методов и средств обеспечения информационной безопасности. **Метод.** В работе предложена трехуровневая модель системы прослеживаемости качества продукции с контролируемым снижением качества и сценарии обеспечения непрерывности ее безопасного функционирования. Базовыми концепциями предлагаемого решения являются: разделение хранимых данных на общедоступные и конфиденциальные; процедуры «отложенного» доверенного предоставления доступа в условиях невозможности непосредственной коммуникации с одним из владельцев данных; разделение данных на шарды — функционально или территориально локализованные хранилища данных; свойства систем распределенного реестра в части обеспечения целостности и доступности данных, неотказуемости операций. **Основные результаты.** Приведены типовые сценарии использования иерархической системы прослеживания качества продукции, сформулировано и предложено решение задачи обеспечения информационной безопасности их реализации. Обосновывается подход к снижению уровня информационной безопасности конкретных реализаций в условиях ресурсных ограничений за счет учета специфики функционирования прикладных систем. Информационная безопасность новых результатов подтверждается компьютерным моделированием с использованием специализированных средств анализа безопасности протоколов. **Обсуждение.** В отличие от известных моделей, ориентированных на использование устойчивых каналов связи, централизованных моделей данных, строгих криптографических алгоритмов и значительных вычислительных ресурсов, не предполагающих получение доступа к данным при отсутствии связи с их владельцем, предлагаемое решение обеспечивает аутентифицированный контролируемый доступ к запрашиваемым конфиденциальным данным и при отсутствии коммуникации с их владельцем. Недостатком реализации рассмотренных сценариев является некоторое снижение уровня информационной безопасности, связанное с делегированием доверия третьей стороне, а также упрощением компрометации шард — узлов распределенного реестра.

Ключевые слова

непрерывность функционирования, конфиденциальная информация, неустойчивая коммуникация, система прослеживаемости качества продукции, предварительная авторизация, доверенная сторона

Благодарности
Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации, соглашение № 075-11-2023-015 от 10.02.2023, «Создание высокотехнологичного серийного производства энергоэффективных синхронных электродвигателей со встроенным интеллектуальным датчиком положения и функциями самодиагностики для робототехники и цифровых систем автоматизации».

Ссылка для цитирования: Лэ В.Х., Комаров И.И., Привалов А.А., Пыркин А.А. Модель обеспечения непрерывности безопасного функционирования системы прослеживаемости качества продукции в условиях неустойчивой коммуникации // Научно-технический вестник информационных технологий, механики и оптики. 2024. Т. 24, № 6. С. 949–961. doi: 10.17586/2226-1494-2024-24-6-949-961

A model for ensuring the continuity of the safe functioning of the product quality traceability system in conditions of unstable communication

Van Hieu Le[1], Igor I. Komarov[2]✉, Aleksandr A. Privalov[3], Anton A. Pyrkin[4]

[1,2,4] ITMO University, Saint Petersburg, 197101, Russian Federation
[3] Federal State Institution of Higher Education "Russian University of Transport" (MIIT), Moscow, 127994, Russian Federation

[1] dragon220294@gmail.com, https://orcid.org/0000-0002-9413-5138
[2] i_krov@mail.ru✉, https://orcid.org/0000-0002-6542-4950
[3] privalov1985@ya.ru, https://orcid.org/0000-0001-8977-152X
[4] a.pyrkin@gmail.com, https://orcid.org/0000-0001-8806-4057

Abstract
Evidence-based technologies for product quality have a positive impact on a wide range of social and economic processes. One of the immanent problems of implementing such technologies is determined by the contradiction between the need to ensure open access to information about the stages of the technological process and the confidentiality of some of such data. The use of strict cryptographic procedures to resolve this contradiction is often impossible due to resource constraints, in particular, the lack of continuous telecommunications between the parties involved. The results obtained are aimed at ensuring the feasibility of product quality traceability systems under resource constraints. They are based on a new architectural solution and the integration of classical methods and tools to ensure information security. The paper proposes a three-level model of a product quality traceability system with controlled quality degradation and scenarios for ensuring the continuity of its safe operation. The basic concepts of the proposed solution are: separation of stored data into publicly available and confidential; procedures for "deferred" trusted access in conditions where direct communication with one of the data owners is impossible; data separation into shards — functionally or geographically localized data warehouses; immanent properties of distributed registry systems in terms of ensuring data integrity and availability, non-repudiation of operations. The paper introduces typical scenarios for the use of a hierarchical product quality tracking system, sets and proposes a solution to the problem of ensuring information security of their implementation. The approach to reducing the level of information security of specific implementations in conditions of resource constraints is justified by taking into account the specifics of the functioning of application systems. The information security of the new results is confirmed by computer modeling using specialized protocol security analysis tools. Unlike well-known models focused on the use of stable communication channels, centralized data models, strict cryptographic algorithms and significant computing resources that do not involve accessing data in the absence of communication with their owner, the proposed solution provides authenticated controlled access to the requested confidential data and in the absence of communication with their owner. An immanent disadvantage of the implementation of the discussed scenarios is a certain decrease in the level of information security associated with delegating trust to a third party as well as simplifying the compromise of distributed registry shard nodes.

Keywords
continuity of operation, confidential information, unstable communication, product quality traceability system, pre-authorization, trusted party

Acknowledgements
The work was supported by the Ministry of Science and Higher Education of the Russian Federation, Agreement No. 075-11-2023-015, 10.02.2023, "Creation of high-tech serial production of energy-efficient synchronous electric motors with integrated intelligent position sensor and self-diagnosis functions for robotics and digital automation systems".

For citation: Le V.H., Komarov I.I., Privalov A.A., Pyrkin A.A. A model for ensuring the continuity of the safe functioning of the product quality traceability system in conditions of unstable communication. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2024, vol. 24, no. 6, pp. 949–961 (in Russian). doi: 10.17586/2226-1494-2024-24-6-949-961

Введение

На системы прослеживаемости качества продукции (СПКП) в развитых экономиках возлагается несколько групп основных задач. Кроме задачи прослеживаемости качества продукции, к ним следует отнести: фискальную[1,2,3] (мониторинг рынка и регулирование обращения отдельных видов товаров и предоставления услуг); конкурентную (создание платформы доказательного подтверждения добросовестности производителя[4]); противодействие фальсификации и предотвращение криминализации бизнесов[5,6,7]. Однако успешное внедрение подобных систем приводит и к ряду косвенных положительных эффектов, например — сохранение здоровья и повышение общего качества жизни населения, стимулирование туристического сектора, ориентированного на локализованные уникальные продукты.

Стандартная архитектура СПКП предполагает взаимодействие причастных сторон в режиме реального времени посредством устойчивых каналов связи, централизованной иерархической модели данных, строгой аутентификации участников процесса. Но даже при выполнении всех этих условий имеют место временные задержки, вызванные как организационными, так и техническими проблемами. Более того, эти сложности отражены в нормативных документах[8], например, предусматривающих возможность задержки предоставления данных в Единую государственную автоматизированную информационную систему учета объема производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции от одного до 7 суток. Очевидно, что такие ограничения могут приводить к нарушению непрерывности функционирования бизнес-процессов, что снижает уровень доверия и готовности к использованию СПКП конечным потребителем.

В условиях развивающихся рынков разработка и внедрение СПКП сталкивается с проблемой обеспечения непрерывной телекоммуникации, ограничением вычислительных ресурсов и недостаточным развитием криптографической инфраструктуры. Таким образом, объективно существует научно-техническая проблема, связанная с принципиальной нереализуемостью СПКП, построенных на классических принципах и технологиях, в условиях ресурсных ограничений, прежде всего связанных с непрерывностью телекоммуникации причастных сторон.

Научная новизна *постановки задачи*, представленной в настоящей работе, состоит во введении дополнительного требования обеспечения доступа к запрашиваемой информации при отсутствии в коммуникационной сети не более одной из сторон, принимавших участие в формировании информационного блока.

Оригинальность *предлагаемого решения* состоит в обеспечении принципиальной возможности реализации СПКП за счет разработки новой архитектуры и адаптации существующих методов и средств обеспечения информационной безопасности (ИБ), в том числе — непрерывности функционирования системы. Снижение уровня ИБ компенсируется проблемно-ориентированной организацией информационных потоков и процедур, основанных на взаимном контроле и конкуренции.

В настоящей работе рассмотрено решение на примере участников рыбопромышленной отрасли Социалистической Республики Вьетнам (СРВ), которая обеспечивает существенную долю доходной части бюджета страны и тесно связана с индустрией туризма [1].

Постановка задачи

Пусть имеется национальная СПКП, интегрированная в расширенную производственную цепочку и содержащая общедоступную и конфиденциальную информации [2, 3]. Основными группами причастных сторон являются: органы-регуляторы (надзорные органы); производители товаров и поставщики услуг, использующие данные товары; конечные потребители товаров и услуг.

С точки зрения обеспечения ИБ формулируются требования: относительно общедоступной информации (обеспечение доступности, целостности (неизменности) внесенных данных и неотказуемости проведенных транзакций); относительно конфиденциальной информации (требования дополняются задачей аутентифицированного доступа по решению владельца информации). Кроме того, могут предъявляться иные требования в рамках концепции интероперабельности сетецентрических информационно-управляющих систем [4].

Система должна обеспечивать контроль качества товара в реальном режиме времени: интерактивно для конечного потребителя, с задержкой до пяти дней (для надзорных органов).

---

[1] ФГИС ВетИС — Федеральная государственная информационная система в области ветеринарии. URL: https://vetrf.ru/ (дата обращения: 28.08.2024).

[2] Единая государственная автоматизированная информационная система Учета древесины и сделок с ней. URL: https://lesegais.ru/ (дата обращения: 28.08.2024).

[3] Лесной кодекс Российской Федерации от 04.12.2006 N 200-ФЗ (ред. от 04.08.2023), Статья 50.6. Единая государственная автоматизированная информационная система учета древесины и сделок с ней.

[4] Приказ Министерства сельского хозяйства РФ от 18.12.2015 г. № 648 «Об утверждении Перечня подконтрольных товаров, подлежащих сопровождению ветеринарными сопроводительными документами» (в редакции приказа Минсельхоза России от 15 апреля 2019 г. № 193).

[5] Федеральная служба по контролю за алкогольным и табачным рынками. Единая государственная автоматизированная информационная система учета объема производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции. URL: https://egais.ru/ (дата обращения: 28.08.2024).

[6] Указ Президента РФ от 08.08.2023 № 587 «О некоторых вопросах государственного управления и контроля в области производства и оборота табачных изделий, табачной продукции, никотинсодержащей продукции и сырья для их производства».

[7] Постановление Правительства РФ от 28.04.2006 N 253 «О требованиях к техническим средствам фиксации и передачи информации об объеме производства и оборота этилового спирта и спиртосодержащей продукции».

[8] Приказ Федеральной службы по регулированию алкогольного рынка от 17.12.2020 № 397.

Сценарии использования системы: основной (при наличии устойчивой телекоммуникации между всеми причастными сторонами); резервный (в условиях отсутствия связи не более, чем с одним из участников).

Метод решения задачи обеспечения непрерывности безопасного функционирования СПКП в условиях неустойчивой коммуникации

Решение поставленной задачи представляется согласованными сценариями безопасного взаимодействия причастных сторон с использованием трехуровневой архитектуры распределенной информационной системы.

Архитектура СПКП и подходы к решению задачи. Предлагаемые решения ориентированы на реализацию функциональных задач СПКП рыбопромышленной отрасли СРВ. Обобщенная архитектура системы предполагает трехуровневую декомпозицию (рис. 1).

Для решения задачи хранения данных предлагается использовать широко известные технологии распределенного реестра (рис. 1, централизованный и локальный уровни СПКП). Исходя из свой концепции, уровни СПКП обеспечивают повышенную по сравнению с централизованными моделями доступность данных (за счет дублирования записей в нескольких узлах), а также целостность данных и неотказуемость операций (за счет применения стека подписаний в конкурирующей среде).

Такое архитектурное решение позволяет обеспечить требования ИБ для общедоступной информации. Однако оно сопряжено с ресурсоемкостью (ввиду вычислительной сложности) обслуживания распределенного реестра.

Для снижения ресурсоемкости применены технологии шардинг-блокчейна [5–7]. Разделение единого распределенного реестра на относительно независимые шарды проводится на основании следующих соображений: территориальная локализация обеспечивает бóльшую вероятность устойчивой коммуникации абонентов, а функциональная декомпозиция — взаимный контроль конкурентов за корректностью данных в шарде. Например, общее количество шард в СПКП рыбопромышленной отрасли СРВ может варьироваться в диапазоне от 300 до 500 шт. на основании следующих данных: общее число провинций — 64 (территориальные шарды); 82 главных рыболовных порта, обеспечивающих прием квотированной продукции (функциональные шарды взаимных конкурентов); 86 рыболовных союзов, объединяющих поставщиков морепродуктов от индустриального до частного масштаба (функциональные шарды).

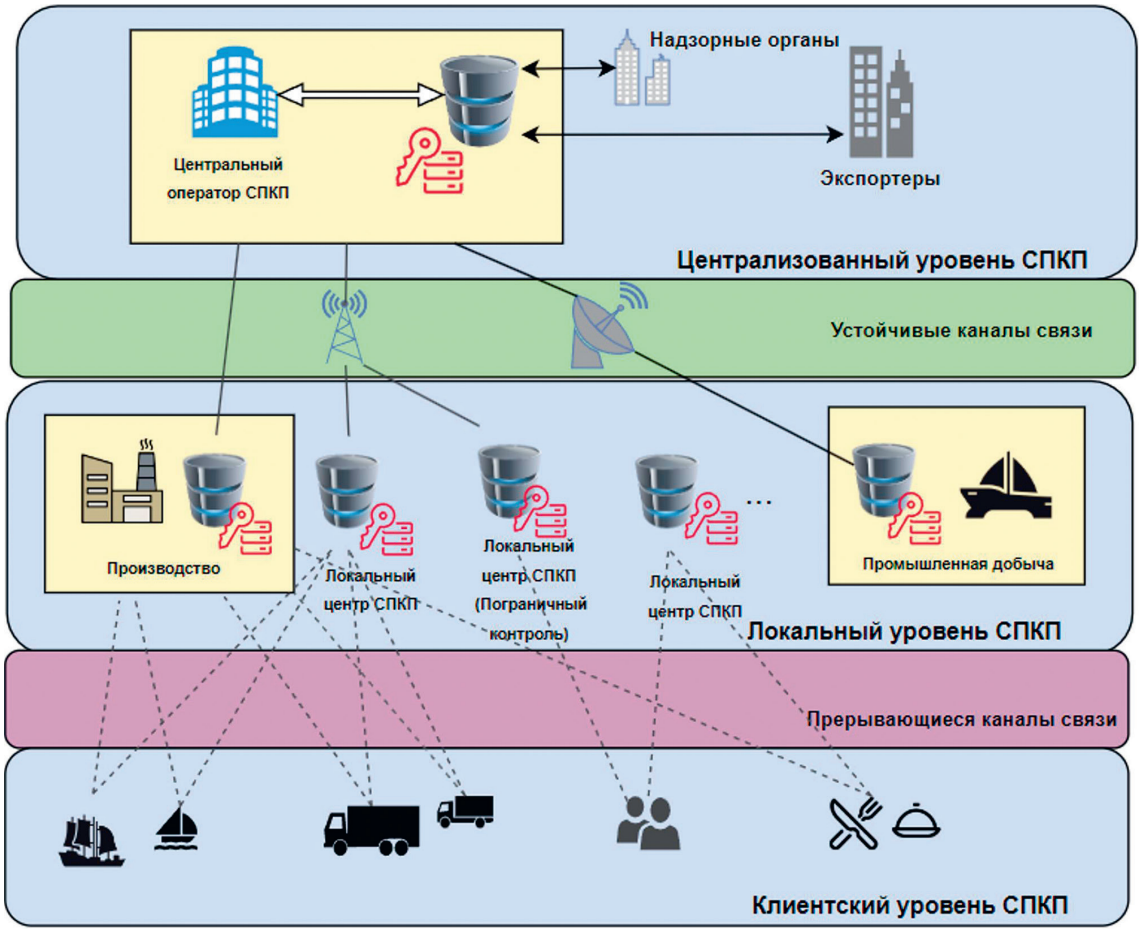


Рис. 1. Обобщенная архитектура системы прослеживаемости качества продукции

Fig. 1. Generalized product quality tracking system architecture

Задача обеспечения ИБ конфиденциальных данных требует иного подхода:

1) разделение общего массива данных на общедоступный и конфиденциальный [2], что снижает количество потребных криптопроцедур;
2) шифрование конфиденциальных данных с использованием криптографического сессионного ключа, обращение с которым реализуется на основе авторского метода [3] с использованием инфраструктуры открытых ключей (Public Key Infrastructure, PKI) и привлечением третьей доверенной стороны;
3) создаются сценарии управления сессионным криптографическим ключом для обеспечения аутентифицированного доступа по решению владельца данных.

Сценарии обеспечения непрерывности безопасного функционирования СПКП. Модель безопасного функционирования СПКП должна обеспечивать безусловное выполнение всех требований ИБ, в том числе переосмысленное в последнее время условие поддержания непрерывности обсуживаемого бизнес-процесса. С учетом принятой концепции разделения публичной и конфиденциальной информации основная роль отводится правилам и сценариям управления симметричным криптографическим ключом, который используется для шифрования данных хранимых транзакций.

Рассмотрим общие правила управления сессионным криптографическим ключом.

Предположим, что стороны (агенты) Agent (A), Business (B), Trast (T) и Client (C) имеют возможность использовать инфраструктуру PKI. Агент T является доверенной третьей стороной, которая помогает управлять ключами и генерирует общие сессионные ключи для шифрования данных по мере необходимости. Агенты A и B совершают транзакцию, и им требуется, чтобы T сгенерировал общий ключ для шифрования конфиденциальных данных в рамках этой транзакции [3].

В стандартных условиях для доступа к этим зашифрованным конфиденциальным данным необходимо разрешение как от A, так и от B. Однако, если A теряет доступ к сети (например, выходя на промысел), T может выступить в качестве посредника, разрешив C доступ к информации совместно с B. Впоследствии T должен уведомить A о выдаче разрешения, когда его соединение будет восстановлено.

Сценарий 1. Отложенная услуга — авторизация и доступ через посредника (рис. 2). Обеспечение единой концепции использования СПКП требует фиксации общей устойчивой точки входа (агент A) для конечного потребителя (агент C), например туриста, включенного в PKI на период действия его визы. Тогда алгоритм

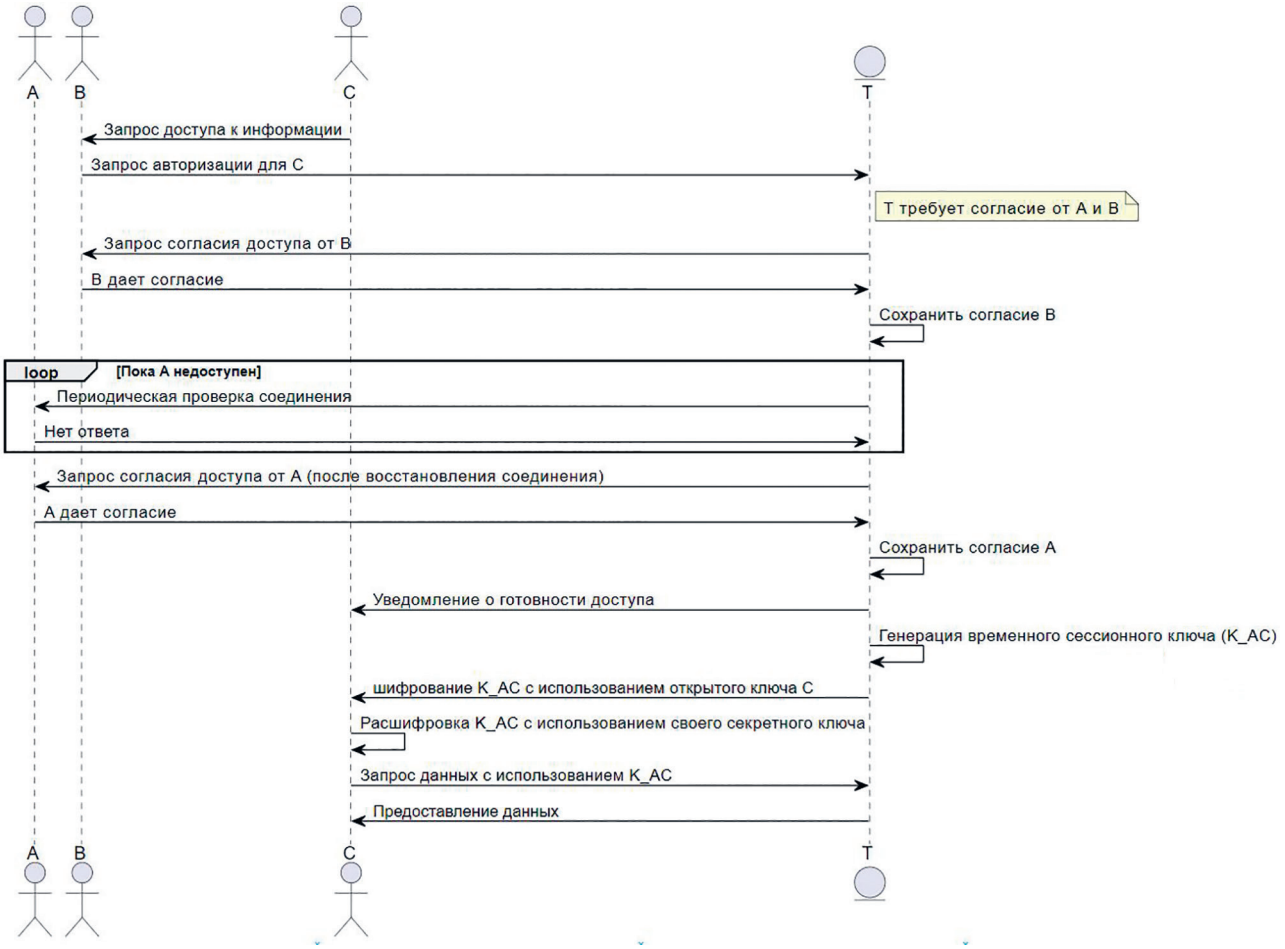


Рис. 2. Сценарий 1 доступа к конфиденциальной информации в режиме отложенной услуги

Fig. 2. Scenario 1 of access to confidential information in the deferred service mode

оффлайн-доступа к конфиденциальным данным предполагает выполнение следующих действий:

— если у агента A пропадает соединение, а C требуется доступ к конфиденциальным данным, B запрашивает у T авторизацию для C;
— T требует разрешения от A и B, чтобы предоставить C доступ к данным;
— так как A отключен, B выдает согласие, и T сохранит его до подключения A;
— как только A восстанавливает соединение, T запрашивает у A разрешение для C;
— агент A выдает разрешение, которое T надежно хранит;
— после получения разрешений от A и B, агент T генерирует временный сессионный ключ (K_AC) для C;
— T шифрует K_AC с использованием публичного ключа C и отправляет ему;
— C расшифровывает это сообщение с использованием своего закрытого ключа и получает K_AC;
— C использует K_AC для временного доступа к конфиденциальным данным;
— T генерирует подтверждение авторизации, включая временную метку и детали предоставленного доступа, подписывает его и отправляет A;
— A получает это подтверждение, как только снова подключается к сети.

Выполнение требований ИБ: конфиденциальность (использование симметричного шифрования на ключе K_AC); целостность (применение цифровых подписей для всех сообщений [8]); аутентификация (достигается средствами PKI); неотказуемость (используются цифровые сертификаты и PKI [9], подписанные доказательством авторизации, предоставленным T агенту A).

Реализация сценария 1 удовлетворяет потребности надзорных органов, однако не соответствует ожиданиям клиента по интерактивному взаимодействию, ввиду непредсказуемости момента восстановления коммуникации с агентом A. Потому целесообразно предусмотреть механизм предварительной авторизации [10] или использовать пороговую криптографию [11, 12] для обеспечения непрерывного доступа к данным без ущерба для ИБ.

Приведем сценарии 2 и 3, которые могут служить решениями поставленной задачи.

Сценарий 2. Интерактивная услуга — механизм предварительной авторизации. Обеспечение непрерывности взаимодействия в условиях отсутствия коммуникации базируется на предварительной генерации

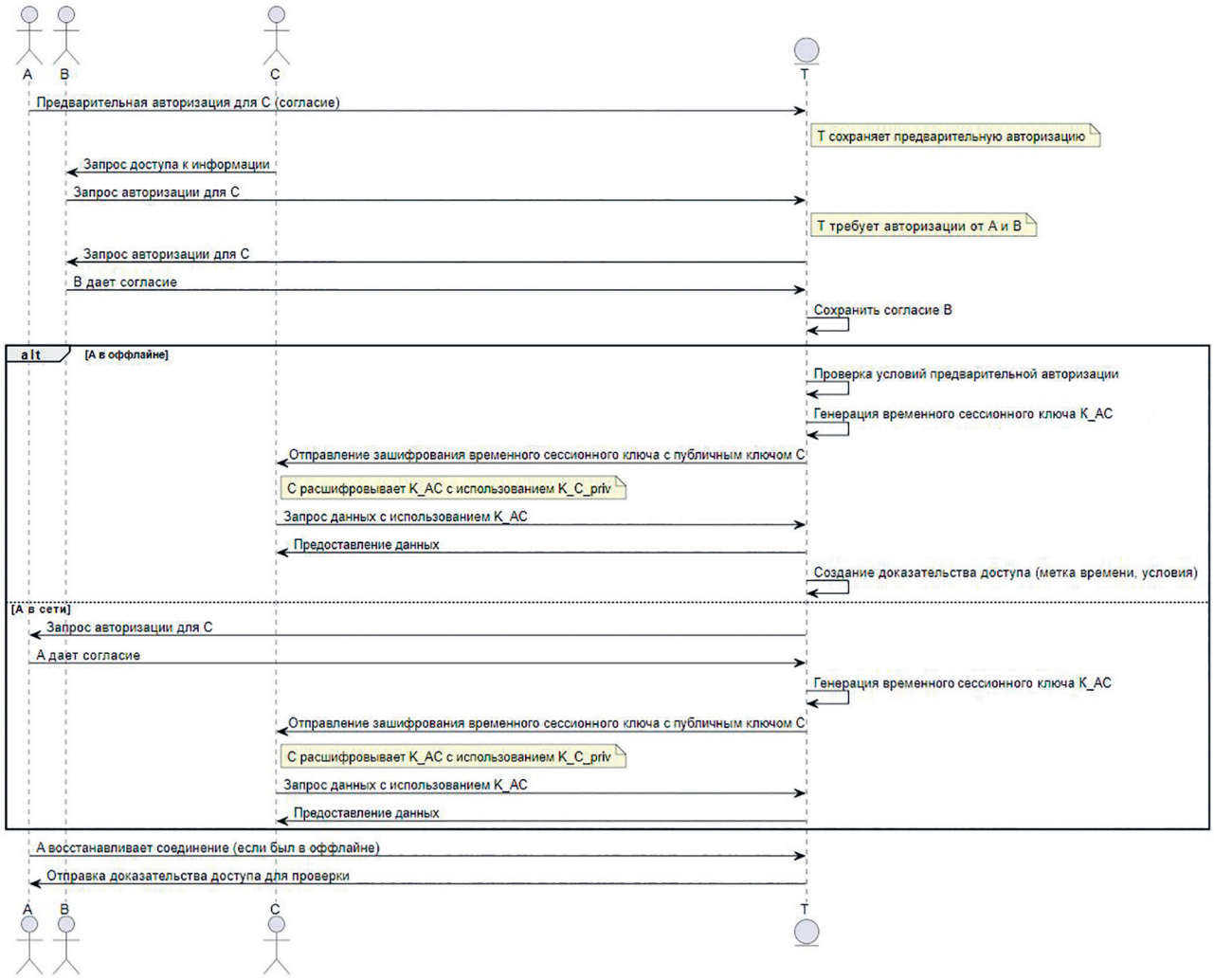


Рис. 3. Сценарий 2 доступа к конфиденциальной информации с использованием механизма предварительной авторизации

Fig. 3. Scenario 2 of access to confidential information using the pre-authorization mechanism

условного согласия агента А — владельца данных на период его недоступности (рис. 3).

На этапе подготовки предварительной авторизации А и В устанавливают политику (набор правил), определяющую, когда, на какой период и при каких условиях С может получить доступ к конкретным данным.

— А и В предварительно авторизуют Т для предоставления доступа С к данным при выполнении этих условий.
— Т безопасно хранит предварительную авторизацию.
— Если С необходимо получить доступ к данным, пока А находится вне связи, Т проверяет условия предварительной авторизации.
— После положительной проверки Т предоставляет С доступ к данным: генерирует K_AC для С, зашифрованный с помощью публичного ключа С и отправляет ему.
— С расшифровывает это сообщение с использованием своего закрытого ключа и получает K_AC.
— С использует K_AC для временного доступа к конфиденциальным данным.
— Т создает, подписывает и хранит уведомление о доступе, включающее метку времени и условия, при которых он был предоставлен.
— Т отправляет уведомление о предоставленном доступе А при его подключении к сети.

Сценарий 3. Интерактивная услуга — пороговая криптография. Еще одним вариантом обеспечения непрерывности функционирования СПКП при условии доверия к третьей стороне является использование пороговой криптографии (рис. 4).

— Используя функционал пороговой криптографии сессионный ключ K_AB разделяется на n частей, и для его восстановления необходимо $k < n$ частей (например, схема разделения секрета Шамира [13–15]). В данном случае он разделен на три части (между агентами А, В и Т), для восстановления нужны любые две из них.
— А, В и Т распределяют и хранят свои части безопасно, обеспечивая невозможность восстановления ключа одним субъектом.
— Когда А теряет соединение, В и Т объединяют свои части для восстановления K_AB.
— Т генерирует K_AC (K_AC генерируется на основе K_AB, но имеет ограничения по времени или области действия), который используется для предоставления агенту С временного доступа к информации.
— Т шифрует K_AC с использованием публичного ключа С и отправляет ему.
— С расшифровывает это сообщение с использованием своего закрытого ключа и получает K_AC.
— С использует K_AC для временного доступа к конфиденциальным данным.
— Как только А снова подключится к сети, Т уведомляет А о том, что сессионный ключ был восстановлен и использован для предоставления доступа С.

Выполнение требований ИБ: конфиденциальность, целостность и неотказуемость обеспечиваются теми же механизмами, которые использованы при обсуждении сценария 1. Дополнительным свойством является обеспечение доступности данных, лежащее в основе непрерывности функционирования СПКП.

Основные результаты

Разработка информационных систем государственного масштаба является сложной научно-технической задачей. Она требует согласованных решений по всем видам обеспечения — от концептуальных политических и правовых до конкретных программно-алгоритмических. Очевидно, что ошибочные решения, принятые на ранних этапах жизненного цикла, ставят под угрозу успешность реализации целевого функционала и саму возможность достижения поставленных целей.

В работе приведено обоснование модели реализации задачи обеспечения непрерывности безопасного функционирования СПКП в условиях неустойчивой коммуникации как одного из ключевых компонентов, который должен обеспечить не только возможность достижения заданного функционала в условиях ресурсных ограничений, но и создать предпосылки для эволюционного развития системы. В существующих условиях неустойчивой коммуникации агентов для реализации предлагаются сценарии 1–3, а при дальнейшем развитии телекоммуникации — переход на модель непрерывного взаимодействия.

Принятие решения об использовании предлагаемой модели должно опираться на достоверные данные о выполнении заданных требований в контексте интероперабельности [4]. Очевидно, что предъявление полного набора требований может привести к невозможности практической реализации системы ввиду ее неприемлемой стоимости, превышающей ожидаемый экономический эффект. Однако верификация безопасности предлагаемых решений в формулировке раздела «Постановка задачи» является обязательной процедурой.

Приведем результаты оценки выполнения требований к ИБ предлагаемых решений на основе компьютерного моделирования.

Одним из подходов к верификации безопасности коммуникационных протоколов, в том числе использующих криптографические средства, является использование теоретико-множественных логических моделей, а также реализующих их специализированных инструментальных средств. В настоящей работе для решения этой задачи применено заслужившее доверие профессионального сообщества инструментальное средство Automated Validation of Internet Security Protocols and Applications (AVISPA) [16, 17].

Действия агентов А, В, С и Т, а также правила и требования к ИБ сценариев по аналогии логических процедур [18] приведены к формату коммуникационных протоколов и формально определены на языке High Level Protocol Specification Language (листинг 1 для сценария 2).

Результаты автоматической проверки (зеленое поле SAFE на рис. 5) демонстрируют безопасность решения в рамках формализованных условий поставленной задачи.

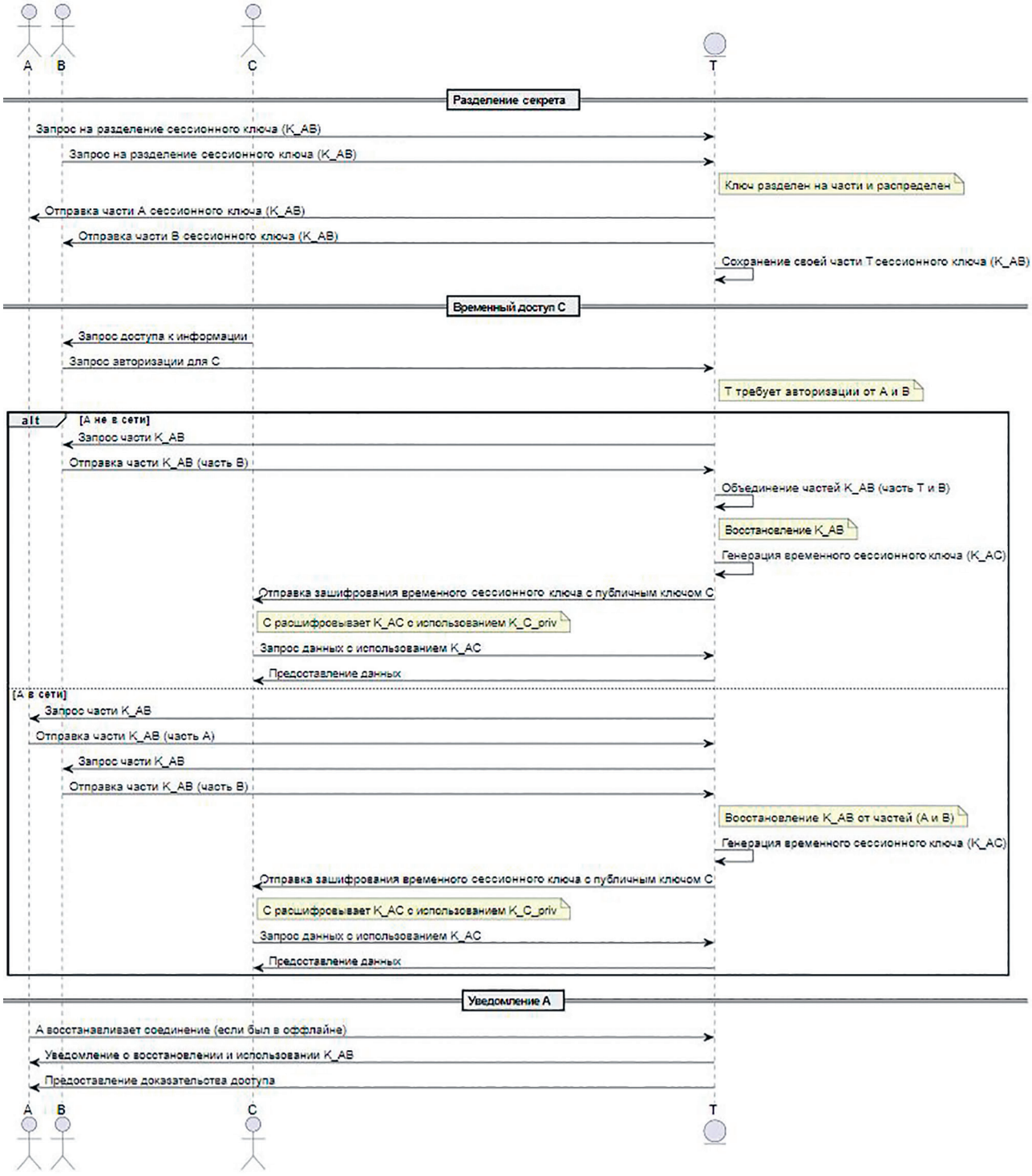


Рис. 4. Сценарий 3 доступа к конфиденциальной информации с использованием пороговой криптографии

Fig. 4. Scenario 3 of access to confidential information using threshold cryptography

Листинг 1. Формализованное описание сценария 2 в среде AVISPA
Listing 1. Formalized description of Scenario 2 in the AVISPA environment

```
Listing 1 Formalized description of Scenario 2 in the AVISPA environment
role client (C,T,B,A:agent,
                    PKc,PKt,PKb:public_key,
                      ST,RT:channel(dy))
 played_by C
 def=
                 local
                             State:nat,
                Nc, Nt:text,
                      K1: symmetric_key
                 init
                             State := 0
              transition
                   1. State  = 0 /\ RT(start) =|>
            State':= 1 /\ Nc' := new()
                                              /\ ST({C.A.B.T.Nc'}_PKt)

                    2. State  = 1 /\ RT({C.B.T.Nc.K1'}_PKc) =|>
                    State':= 2 /\ request(C,T,auth_1,Nc)
end role


 role bob (   B,T,C:agent,
                    PKb,PKt,PKc:public_key,
                      ST,RT:channel(dy))
 played_by B
 def=
                 local
                             State:nat,
                          Nb,Nt,Nc:text
                 init
                             State := 0
               transition
  1. State  = 0 /\ RT({T.C.B.Nt'}_PKb)=|>
              State':= 1 /\ Nb' := new()
                                           /\ ST({T.C.B.Nt.Nb'}_PKt)
                                           /\ witness(B,T,auth_2,Nt)
 end role

role trusted (T,B,C,A:agent,
                    PKt,PKb,PKc:public_key,
                    KeyMap: (agent.public_key) set,
                    SC,RC,SB,RB:channel(dy))
 played_by T
 def=
                 local
                             State:nat,
                           Nc,Nt,Nb:text,
                         K1:symmetric_key
       const sec_1: protocol_id
                 init
                             State := 0
               transition
   1. State  = 0 /\ RC({C.A.B.T.Nc'}_PKt)
                                            /\ in(C.PKc, KeyMap) =|>
               State':= 1 /\ Nt' := new()
                             /\ SB({T.C.B.Nt'}_PKb)
```

```
   2. State  = 1 /\ RB({T.C.B.Nt.Nb'}_PKt)=|>
      State':= 2 /\ request(T,B,auth_2,Nt)
                                          /\ K1' := new()
                                          /\ SC({C.B.T.Nc.K1'}_PKc)
                                          /\ witness(T,C,auth_1,Nc)
                                          /\ secret(K1',sec_1,{C,T,B})
 end role

 role session(C:agent,B:agent,T:agent, A:agent,PKc,PKb,PKt:public_key,
KeySet: agent -> (agent.public_key) set)
 def=
                 local
                    ST1,RT1,SC,RC,SB,RB,ST2,RT2:channel(dy)
               composition
                 client(C,T,B,A,PKc,PKt,PKb,ST1,RT1) /\
                    bob(B,T,C,PKb,PKt,PKc,ST2,RT2) /\
                 trusted(T,B,C,A,PKt,PKb,PKc,KeySet(T),SC,RC,SB,RB)
 end role

 role environment()
 def=
  local KeyMap: (agent.public_key) set
                  const
                    pkc,pkb,pkt,pki:public_key,
                  c,b,t,i,a:agent,
                  sec_1,auth_1,auth_2:protocol_id
      init KeyMap := {b.pkb,t.pkt}
intruder_knowledge = {c,b,t,a,pkc,pkb,pkt,pki,inv(pki)}
               composition
            %% We run the regular session
session(c,b,t,a,pkc,pkb,pkt,{t.{b.pkb,c.pkc},b.{b.pkb},i.{i.pki}})
            %% in parallel with another regular session
         /\ session(c,b,t,a,pkc,pkb,pkt,{t.{b.pkb,c.pkc},b.{b.pkb},i.{i.pki}})
/\ session(i,b,t,a,pki,pkb,pkt,{t.{b.pkb,i.pki},b.{b.pkb},i.{i.pki}})

 end role

goal
           secrecy_of sec_1
        authentication_on auth_1
       authentication_on auth_2
 end goal
 environment()
```

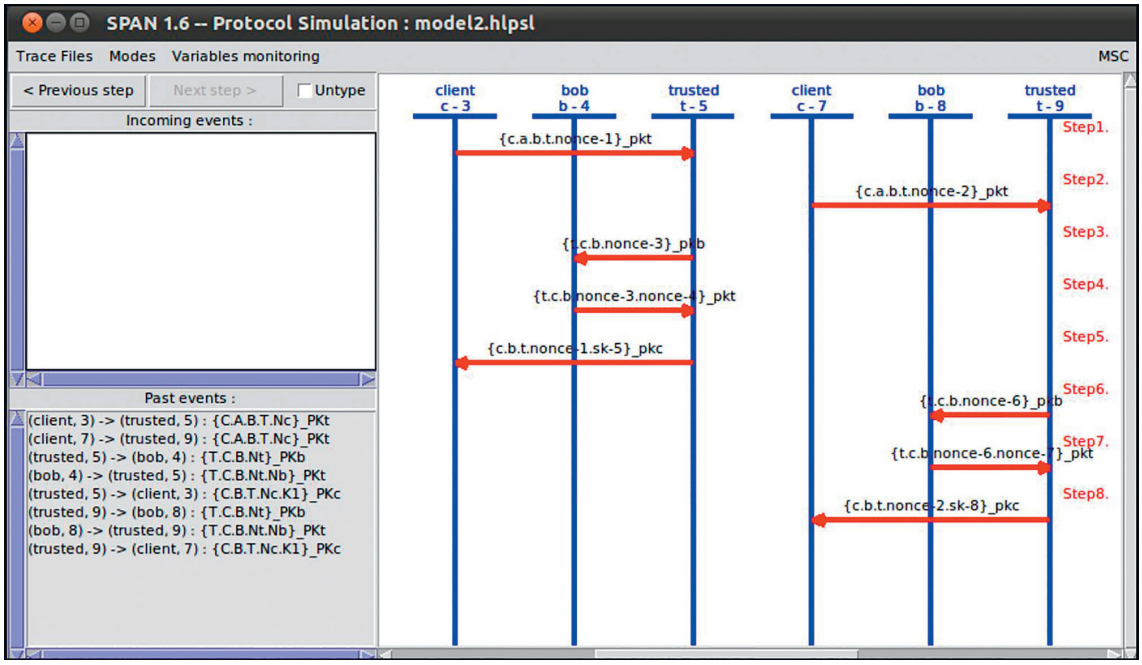
```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/model2.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.28s
 visitedNodes: 415 nodes
 depth: 6 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/model2.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed  : 4 states
 Reachable  : 0 states
 Translation: 0.00 seconds
 Computation: 0.00 seconds
```

Рис. 5. Результаты автоматической проверки безопасности сценария 2 в среде AVISPA

Fig. 5. The results of the automatic security check of Scenario 2 in the AVISPA environment

a



b

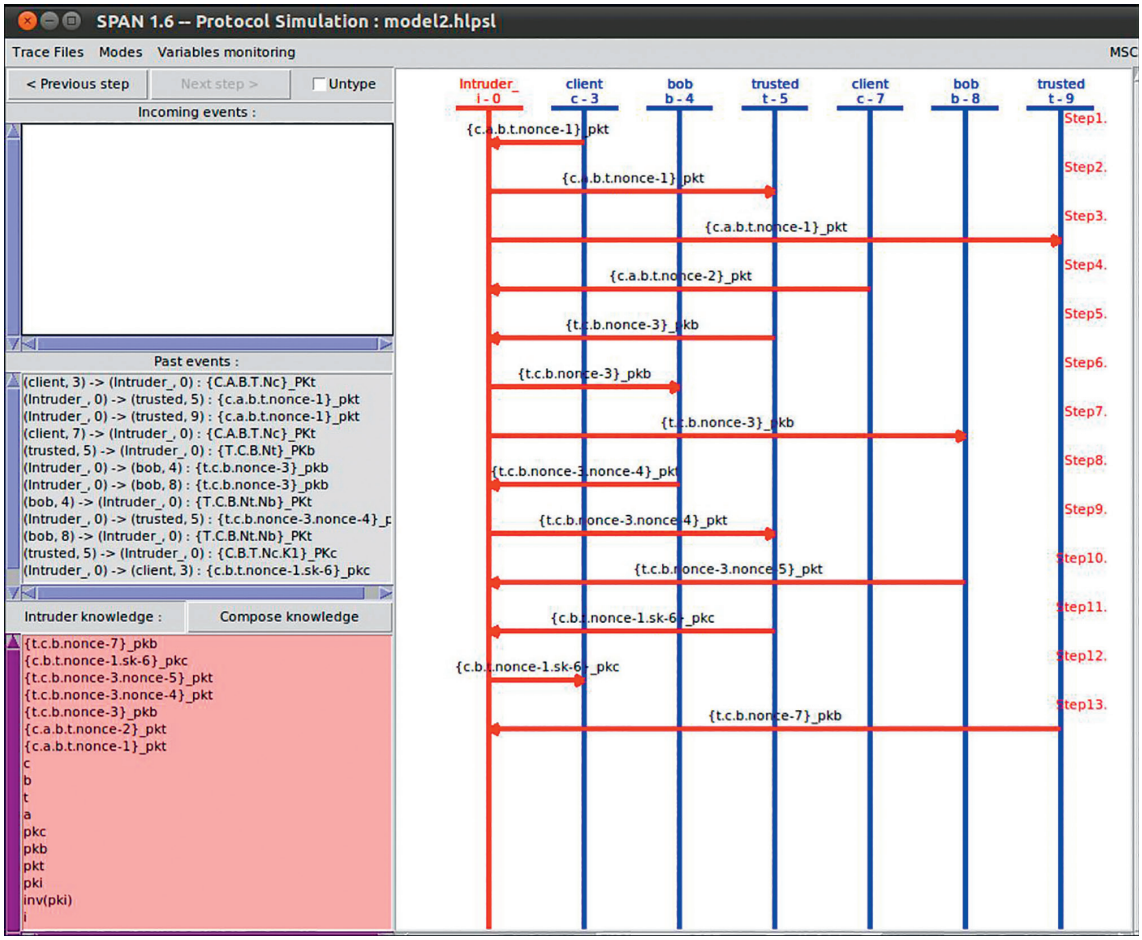


Рис. 6. Визуализация информационных потоков взаимодействия сценария 2 в среде AVISPA: без нарушителя информационной безопасности (*a*); с нарушителем информационной безопасности (*b*)

Fig. 6. Visualization of information flows of interaction Scenario 2 in the AVISPA environment: without an information security violator (*a*); with an information security violator (*b*)

Результаты визуализации информационных потоков (рис. 6), лежащих в основе сценария 2, позволяют сделать вывод о выполнении основных и дополнительных требований ИБ при использовании предлагаемой модели и условии доверия к третьей стороне. Аналогичным образом проведена проверка ИБ сценария 3, подтверждающая выполнение требований, сформулированных в разделе «Постановка задачи».

Заключение

В работе поставлена задача и предложены решения по обеспечению непрерывности функционирования распределенной прикладной информационной системы, использующей в качестве хранилища данных распределенный реестр.

Обеспечение конфиденциальности части данных обеспечивается за счет их шифрования симметричным сессионным ключом. Аутентифицированный доступ к этим данным предполагает предоставление этого ключа на условиях, определяемых владельцами данных.

В отличие от существующих решений, предполагающих непосредственное взаимодействие участников информационного процесса, полученные результаты обеспечивают различные режимы доступа к данным с использованием технологий предварительной аутентификации или пороговой криптографии, в том числе и при невозможности коммуникации с одним из владельцев данных.

Предлагаемые решения требуют наличия третьей доверенной стороны, что порождает дополнительные уязвимости системы. Вместе с тем риски, сопряженные с использованием третьей стороны, не превышают риски, связанные с недобросовестной обработкой данных, а снижение уровня ИБ обеспечивает реализуемость системы в условиях ресурсных ограничений.

Перспективным направлением работы является определение оптимального количества шард-узлов с учетом: различной интенсивности их использования как для предоставления информации, так и для ее пополнения; динамики выхода из зоны непосредственной коммуникации владельцев конфиденциальной информации; затрат на межшардовое взаимодействие; теоретического и экспериментального обоснования влияния внутришардовой конкуренции на вероятность сговора участников для компрометации данных.

Вместе с тем полученные результаты обеспечивают возможность практической реализации системы прослеживаемости качества продукции для Социалистической Республики Вьетнам, ее эволюционное развитие и получение дополнительных данных для ее технической оптимизации.

Литература

1. Лэ В., Бегаев А.Н., Комаров И.И. Модель угроз информационной безопасности системы отслеживания качества продукции для развивающихся рынков // Известия Института инженерной физики. 2024. № 1(71). С. 61–70.
2. Лэ В., Ву Л., Комаров И.И. Обеспечение информационной безопасности в системе прослеживаемости морепродуктов на основе технологии блокчейна // Наука и бизнес: пути развития. 2022. № 5(131). С. 97–101.
3. Лэ В., Бегаев А.Н., Комаров И.И., Фунг В.К. Верификация метода безопасного распределения сессионного ключа в системе отслеживания качества продукции // Вопросы кибербезопасности. 2023. № 6(58). С. 112–121. https://doi.org/10.21681/2311-3456-2023-6-112-121
4. Черницкая Т.Е., Макаренко С.И., Растягаев Д.В. Аспекты информационной безопасности в рамках оценки интероперабельности сетецентрических информационно-управляющих систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2020. № 4. С. 113–121. https://doi.org/10.25586/RNU.V9187.20.04.P.113
5. Liu Y., Liu J., Salles M.V., Zhang Z., Li T., Hu B., Henglein F., Lu R. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems // Computer Science Review. 2022. V. 46. P. 100513. https://doi.org/10.1016/j.cosrev.2022.100513
6. Luu L., Narayanan V., Zheng C., Baweja K., Gilbert S., Saxena P. A secure sharding protocol for open blockchains // Proc. of the 2016 ACM SIGSAC conference on computer and communications security. 2016. P. 17–30. https://doi.org/10.1145/2976749.2978389
7. Yu G., Wang X., Yu K., Ni W., Zhang J.A., Liu R.P. Survey: Sharding in blockchains // IEEE Access. 2020. V. 8. P. 14155–14181. https://doi.org/10.1109/access.2020.2965147
8. Banerjee K., Saha S. Blockchain signatures to ensure information integrity and non-repudiation in the digital era: A comprehensive study // International Journal of Computing and Digital Systems. 2024. V. 16. N 1. P. 1–12.
9. Ayele W.Y. Non-repudiation mechanisms for IoT applications: A systematic literature review: Master Degree Project in Informatics with a Specialization in Privacy, Information Security, and Cyber Security, 2021. 65 p.

References

1. Le V.X., Begaev A.N., Komarov I.I. Information security threat model for product quality tracking systems for emerging markets. *Proceedings of the Institute of Engineering Physics*, 2024, no. 1(71). pp. 61–70. (in Russian)
2. Le V., Vu L., Komarov I.I. Ensuring information security in the seafood traceability system based on blockchain. *Science and Business: Ways of Development*, 2022, no. 5(131), pp. 97–101. (in Russian)
3. Le W.H., Begaev A.N., Komarov I.I., Fung W.K Verification of session key safe distribution method in the product quality traceability system. *Voprosy kiberbezopasnosti*, 2023, no. 6(58), pp. 112–121. (in Russian). https://doi.org/10.21681/2311-3456-2023-6-112-121
4. Chernitskaya T.E., Makarenko S.I., Rastyagaev D.V. Aspects of information assurance within net-centric information and control systems interoperability evaluation. *Bulletin of the Russian New University. Series "Complex Systems: models, analysis and management*, 2020, no. 4, pp. 113–121. (in Russian). https://doi.org/10.25586/RNU.V9187.20.04.P.113
5. Liu Y., Liu J., Salles M.V., Zhang Z., Li T., Hu B., Henglein F., Lu R. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems. *Computer Science Review*, 2022, vol. 46, pp. 100513. https://doi.org/10.1016/j.cosrev.2022.100513
6. Luu L., Narayanan V., Zheng C., Baweja K., Gilbert S., Saxena P. A secure sharding protocol for open blockchains. *Proc. of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 17–30. https://doi.org/10.1145/2976749.2978389
7. Yu G., Wang X., Yu K., Ni W., Zhang J.A., Liu R.P. Survey: Sharding in blockchains. *IEEE Access*, 2020, vol. 8, pp. 14155–14181. https://doi.org/10.1109/access.2020.2965147
8. Banerjee K., Saha S. Blockchain signatures to ensure information integrity and non-repudiation in the digital era: A comprehensive study. *International Journal of Computing and Digital Systems*, 2024, vol. 16, no. 1, pp. 1–12.
9. Ayele W.Y. *Non-repudiation mechanisms for IoT applications: A systematic literature review*: Master degree project in informatics with a specialization in privacy, information security, and cyber security, 2021, 65 p.

10. Tan K.-L., Chi C.H., Lam K.Y. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification // Wireless Networks. 2024. V. 30. N 6. P. 4773–4795. https://doi.org/10.1007/s11276-022-03114-6
11. Blackburn S.R. Combinatorics and threshold cryptography // Combinatorial Designs and their Applications. Routledge, 2023. P. 49–70. https://doi.org/10.1201/9781315139722-3
12. Tan L., Yu K., Yang C., Bashir A.K. A blockchain-based Shamir's threshold cryptography for data protection in industrial internet of things of smart city // Proc. of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G. 2021. P. 13–18. https://doi.org/10.1145/3477084.3484951
13. Abdallah A., Salleh M. Secret sharing scheme security and performance analysis // Proc. of the International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE). 2015. P. 173–180. https://doi.org/10.1109/iccneee.2015.7381357
14. Beimel A. Secret-sharing schemes: A survey // Lecture Notes in Computer Science. 2011. V. 6639. P. 11–46. https://doi.org/10.1007/978-3-642-20901-7_2
15. Tejedor-Romero M., Orden D., Marsa-Maestre I., Junquera-Sanchez J., Gimenez-Guzman J.M. Distributed remote e-voting system based on Shamir's secret sharing scheme // Electronics. 2021. V. 10. N 24. P. 3075. https://doi.org/10.3390/electronics10243075
16. Нестеренко А.Ю., Семенов А.М. Методика оценки безопасности криптографических протоколов // Прикладная дискретная математика. 2022. № 56. С. 33–82. https://doi.org/10.17223/20710410/56/4
17. Басан А.С., Басан Е.С., Ищукова Е.А., Корнилов А.П. Протокол взаимной аутентификации группы объектов с динамической топологией // Вопросы кибербезопасности. 2023. № 4(56). С. 41–52. https://doi.org/10.21681/2311-3456-2023-4-41-52
18. Бабенко Л.К., Писарев И.А. Язык PDA для динамического анализа криптографических протоколов // Вопросы кибербезопасности. 2020. № 5(39). С. 19–29. https://doi.org/10.21681/2311-3456-2020-05-19-29

10. Tan K.-L., Chi C.H., Lam K.Y. Secure and privacy-preserving sharing of personal health records with multi-party pre-authorization verification. *Wireless Networks*, 2024, vol. 30, no. 6, pp. 4773–4795. https://doi.org/10.1007/s11276-022-03114-6
11. Blackburn S.R. Combinatorics and threshold cryptography. *Combinatorial Designs and their Applications. Routledge*, 2023, pp. 49–70. https://doi.org/10.1201/9781315139722-3
12. Tan L., Yu K., Yang C., Bashir A.K. A blockchain-based Shamir's threshold cryptography for data protection in industrial internet of things of smart city. *Proc. of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G*, 2021, pp. 13–18. https://doi.org/10.1145/3477084.3484951
13. Abdallah A., Salleh M. Secret sharing scheme security and performance analysis. *Proc. of the International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE)*, 2015, pp. 173–180. https://doi.org/10.1109/iccneee.2015.7381357
14. Beimel A. Secret-sharing schemes: A survey. *Lecture Notes in Computer Science*, 2011, vol. 6639, pp. 11–46. https://doi.org/10.1007/978-3-642-20901-7_2
15. Tejedor-Romero M., Orden D., Marsa-Maestre I., Junquera-Sanchez J., Gimenez-Guzman J.M. Distributed remote e-voting system based on Shamir's secret sharing scheme. *Electronics*, 2021, vol. 10, no. 24, pp. 3075. https://doi.org/10.3390/electronics10243075
16. Nesterenko A.Yu., Semenov A.M. Methodology for assessing the security of cryptographic protocols. *Prikladnaya Diskretnaya. Matematika*, 2022, no. 56, pp. 33–82. (in Russian). https://doi.org/10.17223/20710410/56/4
17. Basan A.S., Basan E.S., Ishchukova E.A., Kornilov A.P. Protocol for mutual authentication of an object's group with dynamic topology. *Voprosy kiberbezopasnosti*, 2023, no. 4(56), pp. 41–52. (in Russian). https://doi.org/10.21681/2311-3456-2023-4-41-52
18. Babenko L.K., Pisarev I.A. PDA language for dynamic analysis of cryptographic protocols. *Voprosy kiberbezopasnosti*, 2020, no. 5(39), pp. 19–29. (in Russian). https://doi.org/10.21681/2311-3456-2020-05-19-29

Авторы

Лэ Ван Хиеу — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-9413-5138, dragon220294@gmail.com
Комаров Игорь Иванович — кандидат физико-математических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 57190606510, https://orcid.org/0000-0002-6542-4950, i_krov@mail.ru
Привалов Александр Андреевич — кандидат технических наук доцент, Российский университет транспорта, Москва, 127994, Российская Федерация, https://orcid.org/0000-0001-8977-152X, privalov1985@ya.ru
Пыркин Антон Александрович — доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 26656070700, https://orcid.org/0000-0001-8806-4057, a.pyrkin@gmail.com

Authors

Van Hieu Le — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-9413-5138, dragon220294@gmail.com
Igor I. Komarov — PhD (Physics & Mathematics), Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 57190606510, https://orcid.org/0000-0002-6542-4950, i_krov@mail.ru
Aleksandr A. Privalov — PhD, Associate Professor, Federal State Institution of Higher Education "Russian University of Transport" (MIIT), Moscow, 127994, Russian Federation, https://orcid.org/0000-0001-8977-152X, privalov1985@ya.ru
Anton A. Pyrkin — D.Sc., Full professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 26656070700, https://orcid.org/0000-0001-8806-4057, a.pyrkin@gmail.com

Статья поступила в редакцию 05.07.2024
Одобрена после рецензирования 20.09.2024
Принята к печати 27.11.2024

Received 05.07.2024
Approved after reviewing 20.09.2024
Accepted 27.11.2024