ВЕРИФИКАЦИЯ МЕТОДА БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ СЕССИОННОГО КЛЮЧА В СИСТЕМЕ ОТСЛЕЖИВАНИЯ КАЧЕСТВА ПРОДУКЦИИ

Лэ В. Х.[1], Бегаев А.Н.[2], Комаров И.И.[3], Фунг В.К.[4]

Цель работы: *определение требований по обеспечению основных и дополнительных свойств информационной безопасности при взаимодействии контрагентов в информационных системах, связанных с обеспечением прослеживаемости качества продукции; разработка и формальная верификация метода генерации и безопасного распределения сессионного ключа, отвечающего этим требованиям.*

Результат: *Использование систем прослеживаемости качества товара является мощным инструментом для решения широкого спектра технологических и социальных задач, например: государственный контроль в регулируемых сферах, обеспечение безопасности потребителя, формирование конкурентного преимущества производителя и т. д. Однако, широкое внедрение таких децентрализованных систем сопряжено с рядом противоречий, одно из которых непосредственно связано с проблемой обеспечения конфиденциальности данных и необходимостью их контролируемого использования в динамическом составе контрагентов и потребителей.*

В работе предлагается направление по преодолению этого противоречия путём формирования сценариев получения контролируемого доступа к приватной информации взаимодействующей стороны с использованием криптографических процедур.

Для реализации таких сценариев разработан метод и базирующийся на нем протокол генерации и распределения секретного сессионного ключа с использованием доверенной третьей стороны. Приводится формальное доказательство безопасности предлагаемого решения с использованием специализированного инструментального средства верификации протоколов.

Полученные результаты в первую очередь ориентированы на применение в системах распределённого реестра, предполагающих разделение данных на приватные и публичные блоки. Однако они могут найти применение и в других системах, предъявляющих требования конфиденциальности, доступности и недоказуемости, особенно при наличии ограничений на вычислительные ресурсы.

Научная новизна: *заключается в проблемно-ориентированном анализе специфических требований по обеспечению информационной безопасности процесса внесения и извлечения данных в систему отслеживания качества товаров в заданных сценариях её использования. На основании выделенных требований формулируется и решается задача разработки адаптированного метода генерации и распределения секретного сессионного ключа между двумя абонентами с привлечением доверенной стороны. На базе разработанного метода синтезируется применимый на практике коммуникационный протокол и проводится формальное доказательство выполнения заданных требований по информационной безопасности, устойчивость к атакам типа «MITM» и повтора.*

Вклад авторов: *Бегаев А.Н. – анализ функциональных потребностей в процессе реализации прикладных распределённых защищённых систем, обоснование научно-методических проблем, определение требований и сценария применения технических решений, базирующихся на новом научном результате; Комаров И.И. – определение методологического противоречия и подхода к его разрешению, определение требований к научному результату, разработка плана исследования; Лэ В. Х. – разработка метода безопасного распределения сессионного ключа в системах отслеживания качества продукции, формализация разработанного метода в тер-*

1 Лэ Ван Хиеу, аспирант факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: hieule250715@gmail.com

2 Бегаев Алексей Николаевич, кандидат технических наук, профессор Университета ИТМО, генеральный директор АО «Эшелон – Северо-Запад», Санкт-Петербург, Россия. E-mail: begaev@mail.ru

3 Комаров Игорь Иванович, кандидат физико-математических наук, доцент, доцент факультета безопасности информационных технологий, Университет ИТМО, Санкт-Петербург, Россия. E-mail: i_krov@mail.ru

4 Фунг Ван Кю, аспирант факультета программной инженерии и компьютерной техники, Университет ИТМО, Санкт-Петербург, Россия. E-mail: hieule250715@mail.com

минах высокоуровневого языка спецификации протоколов, определение ограничений и перспектив развития полученных результатов; Фунг В. К. – проведение эксперимента с помощью специализированного автоматизированного средства верификации безопасности протоколов, визуализация и интерпретация результатов.

Ключевые слова: *кибербезопасность, конфиденциальность, неотказуемость, сессионный криптографический ключ, распределённый реестр, формальная верификация протокола.*

DOI:10.21681/2311-3456-2023-6-112-121

Введение

Теоретическая модель систем распределённого реестра, ставшая основой широко применяющейся блокчейн-технологии, с точки зрения информационной безопасности обеспечивает несколько ключевых свойств хранимых данных. В первую очередь это целостность и неотказуемость. Вместе с тем использование технологии блокчейн сопряжено с высокой вычислительной сложностью и, следовательно, высокой стоимостью требуемых вычислительных средств для обеспечения доступности данных. Одновременно стоит вопрос об обеспечении заданного уровня конфиденциальности информации в реальных производственных цепочках, связанных со взаимодействием различных контрагентов.

Несмотря на пессимистические прогнозы, касающиеся защищённости прикладных систем на основе распределённого реестра в условиях квантовых вычислений [1, 2], считается целесообразным [3-5] продолжение работ в области автоматизации взаимодействия как производителей, так и потребителей в рамках расширенной производственной цепочки.

На примере системы отслеживания качества товара [6], а также ряда других перспективных информационных систем [7-9], предъявляющих специфические требования к процессу информационного взаимодействия, выделяется несколько групп противоречий, требующих разрешения, а именно: противоречие между различным уровнем конфиденциальности данных и единым алгоритмом доступа к ним, а также противоречие между потребностью оперативного получения целостных и аутентичных данных и высокой ресурсоёмкостью этого процесса. Одним из путей практического разрешения указанных противоречий является определение баланса в единой системе прослеживаемости качества товара за счёт использования различных моделей безопасности [10 - 12] для выполнения частных подзадач.

Предпосылки исследования

Работа базируется на достаточно широко известных исследованиях, последовательно развивающих концепцию распределённого реестра для применения в различных отраслях.

Так, Yingwen Chen и др. [13] предложена система, которая использует блокчейн консорциума Hyperledger Fabric для хранения зашифрованных медицинских данных и соответствующих политик контроля доступа. Для защиты конфиденциальности медицинских данных система использует комбинацию K-анонимности и методов шифрования с возможностью поиска. Она также обеспечивает управление доступом на основе атрибутов ABAC (Attribute-Based Access Control) для медицинских данных, что позволяет авторизованным пользователям получать доступ к данным на основе их атрибутов, таких как их роль, отделение и специальность. Однако используемая модель K-анонимности может быть уязвима для атак, если злоумышленник имеет доступ к дополнительной информации о пациентах, такой как их демографические данные или история болезни.

Zheng B.K. и др. [14] предлагают модели шифрования данных и управления ключами для повышения конфиденциальности в блокчейне. В их работе приводится пример применения к блокчейну криптосистемы Пайе, позволяющей защитить конфиденциальную информацию и решить проблему защиты конфиденциальности блока блокчейна. Потенциальная проблема схемы заключается в том, что она использует архитектуру с двумя блокчейнами. Это может увеличить сложность и стоимость системы. Кроме того, безопасность системы зависит от безопасности как общедоступных, так и частных блокчейнов. В работе остался без рассмотрения вопрос функционального (с учётом бизнес-логики процессов) разделения данных по уровням конфиденциальности.

Yang Y. и др. [15] рассматривают вопрос применения безопасных многосторонних вычислений SMPC (Secure Multi-Party Computation) с целью повышения конфиденциальности при совместном использовании данных между несколькими сторонами. При этом отмечается, что реализация безопасных многосторон-

них вычислений ограничена из-за неэффективного, сложного протокола вычислений и частого взаимодействия. Авторы базируются на особенности SMPC, позволяющей нескольким сторонам вычислять функцию на своих частных входных данных, не раскрывая эти входные данные друг другу или какой-либо третьей стороне. Позволяя сторонам совместно обрабатывать конфиденциальные данные, не раскрывая их другим, SMPC может помочь обеспечить безопасность и надёжность системы, в том числе в условиях реализации ряда потенциальных атак. Реализация схема Block-SMPC опирается на безопасность сети блокчейн. Естественным направлением совершенствования обсуждаемой системы является снижение вычислительной сложности протоколов для. большого числа участников.

Как показано в работе[5] коллектива авторов, одной из ключевых уязвимостей информационной безопасности распределённых систем является увеличение числа скомпрометированных элементов, участвующих в совместном обеспечении информационной безопасности, что ещё раз подтверждает требование обеспечения взаимного доверия как друг к другу, так и к совместно генерируемым ресурсам.

Сильные стороны каждого из упомянутых подходов можно использовать для повышения конфиденциальности приватных данных в системах отслеживания на основе блокчейна. В зависимости от конкретных потребностей и требований системы может подойти один или комбинация нескольких из них.

В работе [6] предложена модель повышения безопасности частной информации в системе отслеживания товаров за счёт классификации и разделения доказательно целостного массива на публичные и приватные блоки данных, обеспечивающие решение различных задач в системе прослеживаемости качества товара. Предполагается, что частная информация каждой транзакции будет зашифрована с помощью симметричного ключа, сгенерированного смарт-контрактом. В соответствии с классическими положениями криптографии информационная безопасность защищаемых блоков определяется безопасностью этого ключа. Авторы предлагают метод его защиты путём шифрования с помощью открытых ключей каждой из вовлечённых сторон и последующего сохранения в блокчейне.

5 Дранник А.Л., Егоров Д. А., Коваленко М. Е., Масленников О. С., Комаров И.И. Юрьева Р.А. Исследование деструктивного воздействия роботов-злоумышленников на эффективность работы мультиагентной системы // Процессы управления и устойчивость. – 2014. – Т. 1. – №. 1. – С. 336–340

В настоящей работе приводится метод и формальная верификация протокола использования инфраструктуры открытых ключей для обеспечения доступа к заданному информационному блоку, что обеспечивает соблюдение требований конфиденциальности и снижает ресурсоёмкость операции.

Постановка задачи и модель использования

Пусть в рамках системы прослеживаемости качества товаров двум сторонам (*A* и *B*) нужен общий секретный ключ *K*, сгенерированный доверенным сервером для шифрования их личных данных в каждой транзакции.

Требования:

- должна быть обеспечена взаимная аутентификация ранее «незнакомых» сторон *A* и *B*;
- ключ *K* должен быть секретным;
- протокол обмена ключами *K* должен быть безопасным;
- должна быть обеспечена защищённость от атак типа MITM (Man In The Middle) и повтора;
- используются открытые каналы взаимодействия.

Для решения поставленной задачи предлагается следующий *метод*, который лежит в основе протокола взаимной аутентификации и распределения ключей, основанный на асимметричных криптосхемах. Пусть имеется два заинтересованных контрагента *Alice* и *Bob*, а также третья сторона *Trent*, которой они оба доверяют.

Alice генерирует случайное число *Na* и, зашифровав свой идентификатор (*A*) и это число с открытым ключом *Bob*, и отправляет их *Bob*.

$$Alice \rightarrow \{E_{K_B}(A, Na)\} \rightarrow Bob \qquad (1)$$

Bob: расшифровывает полученное сообщение, извлекает отправленное число Na, генерирует случайное число *Nb* и, зашифровав свой идентификатор (*B*), это число и случайное число Na открытом ключом *Alice* и отправляет *Alice.*

$$Bob \rightarrow \{E_{K_A}(B, Na, Nb)\} \rightarrow Alice \qquad (2)$$

Alice отправляет *Bob* случайные числа, зашифровав сообщение открытом ключом *Bob.*

$$Alice \rightarrow \{E_{K_B}(Na, Nb)\} \rightarrow Bob \qquad (3)$$

Bob отправляет *Trent* оба идентификатора и случайные числа, шифруя его открытом ключом *Trent*.

$$Bob \rightarrow \{E_{K_T}(A, B, Na, Nb)\} \rightarrow Trent \qquad (4)$$

Trent расшифровывает сообщения от *Bob*, узнаёт идентификаторы и случайные числа участников, после чего генерирует сессионный ключ K и отправляет *Bob* два сообщения:

— в первом сообщении содержатся: идентификатор *Bob* (*B*), оба случайных числа (Na, Nb) и сессионный ключ (*K*), зашифрованные на открытом ключе *Alice*;

— во втором сообщении содержатся: идентификатор *Alice* (*A*), оба случайных числа (Na, Nb) и сессионный ключ (*K*), зашифрованные на открытом ключе *Bob*:

$$Trent \rightarrow \{E_{K_A}(B, Na, Nb, K), E_{K_B}(A, Na, Nb, K)\} \rightarrow Bob \quad (5)$$

Bob отправляет *Alice* два сообщения:

1) это сообщение (5), полученное от *Trent*;

2) оба случайных числа, зашифрованные на сессионном ключе:

$$Bob \rightarrow \{E_{K_A}(B, Na, Nb, K), \quad (6)$$

Alice расшифровывает первое сообщение, получает ключ K, расшифровывает второе сообщение и отправляет *Bob* его случайное число:

$$Alice \rightarrow \{E_K(Nb)\} \rightarrow Bob \quad E_K(Na, Nb)\} \rightarrow Alice \quad (7)$$

Таким образом задача генерации и безопасного распределения симметричного сессионного ключа решена при выполнении условия доверия к третьему лицу.

Моделирование протокола и анализ полученных результатов

Принятый авторами подход к верификации предлагаемого метода базируется на известных концепциях[6], получивших подтверждение и развитие в современных работах [16, 17,18, 19], и использует предположение о корректности преобразований следующих элементов: *метод → протокол → алгоритм → формальное описание→ автоматическая верификация в специализированной среде → результат*.

Для моделирования и верификации безопасности протокола взаимодействия трех сторон, базирующегося на предложенном *методе* (1–7), в работе использовано специализированное инструментальное средство AVISPA (Automated Validation of Internet Security Protocols and Applications)[7] с поддержкой языка HLPSL (High Level Protocol Specification Language).

AVISPA — это расширяемый модульный инструмент для автоматической проверки протоколов и приложений (рис. 1). Он использует язык HLPLS для формализованного описания безопасности тестируемых протоколов, набор инструментов для их формальной проверки и модели широко распространённых интерфейсов.

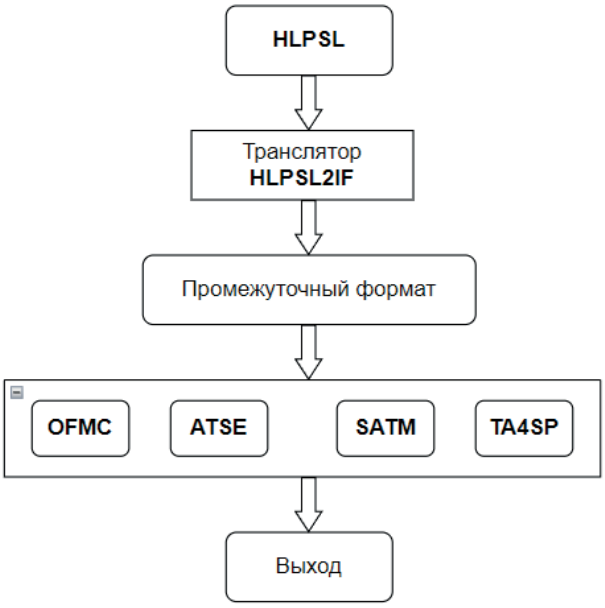

Рис. 1. Упрощённая архитектура инструментального средства AVISPA

OFMC и CL-AtSe — формализованные компоненты для анализа безопасности криптографических протоколов: OFMC ориентирован на проверку общих свойств безопасности, таких как аутентификация и секретность: модуль CL-AtSe целесообразно использовать для анализа конкретных атак.

Выбор инструментального средства определяется прежде всего: доверием профессионального сообщества, доказуемостью, удобством и наглядностью интерпретации результатов, гибкостью языка и доступностью самого инструментального средства.

В настоящей работе протокол взаимной аутентификации и распределения ключей проверен с использованием модулей OFMC и ATSE.

В исследуемом протоколе (1–7) взаимодействуют

6 И. В. Котенко, С. А. Резник, А. В. Шоров, Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств, Тр. СПИИРАН, 2009, выпуск 8, 292–310

7 AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language. Available. URL: https://www.avispa-project.org/(дата обращения 30.08.2023).

```
role role_A(A,B,T       :agent,
            PKa,PKb,PKt : public_key,
            SND,RCV     : channel(dy))
played_by A
def=
        local
                State:nat,
                Na, Nb,Nas:text,
                K: symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV(start) =|>
           State':= 1   /\ Na' := new() /\ SND({A.Na'}_PKb)

        2. State  = 1   /\ RCV({B.Nb'.Na}_PKa)
                        /\ request(A,B,alice_bob_na,Na) =|>
           State':= 2   /\ SND({Na.Nb'}_PKb)
                        /\ witness(A,B,bob_alice_nb,Nb')
        3. State  = 2   /\ RCV({B.Na.Nb.K'}_PKa.{Na.Nb}_K') =|>
           State':= 3   /\ SND({Nb}_K')
                        /\ witness(A,B,bob_alice_k,K')
end role
```

```
role role_B(B,A,T       : agent,
            PKb,PKa,PKt : public_key,
            SND,RCV     : channel(dy))
played_by B
def=
        local
                State:nat,
                Na,Nb:text,
                K:symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV({A.Na'}_PKb) =|>
           State':= 1   /\ Nb' := new() /\ SND({B.Nb'.Na'}_PKa)
                        /\ witness(B,A,alice_bob_na,Na')

        2. State  = 1   /\ RCV({Na.Nb}_PKb)
                        /\ request(B,A,bob_alice_nb,Nb) =|>
           State':= 2   /\ SND({A.B.Na.Nb}_PKt)

        3. State  = 2   /\ RCV({B.Na.Nb.K'}_PKa.{A.Na.Nb.K'}_PKb)
                        /\ request(B,T,bob_trusted_nb,Nb) =|>
           State':= 3   /\ SND({B.Na.Nb.K'}_PKa.{Na.Nb}_K')

        4. State  = 3   /\ RCV({Nb}_K) =|>
           State':= 4   /\ request(B,A,bob_alice_k,K)
end role
```

```
role role_T(T,A,B       :agent,
            PKt,PKa,PKb :public_key,
            SND,RCV     :channel(dy))
played_by T
def=
        local
                State:nat,
                Na,Nb:text,
                K:symmetric_key

        init    State := 0
        transition
        1. State  = 0   /\ RCV({A.B.Na'.Nb'}_PKt) =|>
           State':= 1   /\ K' := new()
                        /\ SND({B.Na'.Nb'.K'}_PKa.{A.Na'.Nb'.K'}_PKb)
                        /\ witness(T,B,bob_trusted_nb,Nb')
                        /\ secret(K',sec_1,{A,B,T})

end role
```

Рис. 2. Описание протокола взаимодействия агентов на языке HLPSL

3 агента *A* (*Alice*), *B (Bob*) и T (*Trent*). Формализованное описание действий агентов на языке HLPSL представлено на рис. 2.

Согласно условиям функционирования требованиями к протоколу являются: секретность данных, взаимная аутентификация агентов и защита от некоторых атак. Формализованное описание целей в терминах AVISPA представлено на рис. 3.

```
goal
        % Secrecy of the key
        secrecy_of sec_1
        % Agent A authenticates agent B
        authentication_on alice_bob_na
        % Agent B authenticates agent A
        authentication_on bob_alice_nb
        authentication_on bob_alice_k
        % Agent B authenticates agent T
        authentication_on bob_trusted_nb
end goal
```

Рис. 3. Цели протокола аутентификации

Параллельные процедуры взаимодействия показаны в «роли среды» (рис. 4), в которой злоумышленник может осуществить атаку.

В результате подготовительных процедур (рис. 2–4) завершено формирование исходных данных для проведения автоматического модельного эксперимента по оценке заданных требований информационной безопасности исследуемого протокола.

Результаты моделирования с использованием модулей OFMC и ATSE представлены на рис.5.а и 5.б соответственно: исследуемый протокол в рамках описанных формализмов и заданных типов атак безопасен (SUMMARY: SAFE). Защита от атак повтора обеспечивается уникальностью случайных чисел (Na, Nb), генерируемых (1, 2) в процессе взаимодействия.

На рис. 6 представлено графическое представление процесса моделирования последовательного взаимодействия между агентами *A*, *B* и *T*.

```
role environment()
def=
        const
                pka,pkb,pki,pkt:public_key,
                alice,bob,trusted:agent,
                sec_1,alice_bob_na,bob_alice_nb,bob_alice_k,bob_trusted_nb:protocol_id
        intruder_knowledge = {alice,bob,trusted,pka,pkb,pkt,pki,inv(pki)}
        composition
                %% We run the regular session
                session(alice,bob,trusted,pka,pkb,pkt)
                %% in parallel with another regular session
                /\ session(alice,bob,trusted,pka,pkb,pkt)
                %% and a session between the intruder  and bob
                /\ session(i,bob,trusted,pki,pkb,pkt)
                %% and a session between alice and the intruder)
                /\ session(alice,i,trusted,pka,pki,pkt)
end role
```

Рис. 4. Описание среды взаимодействия агентов.

```
% OFMC
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/keyExchange8.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 11.44s
  visitedNodes: 10608 nodes
  depth: 10 plies
```

А

а)

```
% ATSE
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/keyExchange8.if

GOAL
  As_specified

BACKEND
  CL-AtSe

STATISTICS
  Analysed : 24 states
  Reachable : 4 states
  Translation : 0.00 seconds
  Computation : 0.00 seconds
```

Б

б)

Рис. 5. Результаты проверки на модуль OFMC и ATSE

Диаграмма взаимодействия, с учётом возможностей атакующего (сторона *Intruder)* по реализации атаки типа MITM, представлена на рис. 7. Переход осуществляется из поля «входящие события» в «прошедшие события». Результаты моделирования в инструменте AVISPA иллюстрирует, что, хотя злоумышленник и перехватил сообщение, секретная информация осталась для него недоступной.

На основе анализа полученных данных формулируется вывод: исследуемый протокол взаимной аутентификации и распределения ключей является безопасным, обеспечивающим выполнение требований (целей) безопасности, установленных на этапе формализации требований к методу: безопасность данных, взаимная аутентификация стороны, защита от повторных атак, атаки MITM.

Применение протокола не требует вовлечения контрагентов в единую инфраструктуру открытых ключей, достаточным условием является попарное доверие к третьей промежуточной стороне. Это обеспечивает возможность взаимодействия контрагентов из различных нормативно-регуляторных, национальных и территориальных зон.

Заключение

В работе поставлена и решена задача разработки *метода* генерации и распределения симметричного сессионного ключа, устойчивого к атакам типа MITM и повтора, для двух контрагентов с использованием доверенной третьей стороны.

Проведено формализованное доказательства безопасности реализующего его *протокола* в задан-

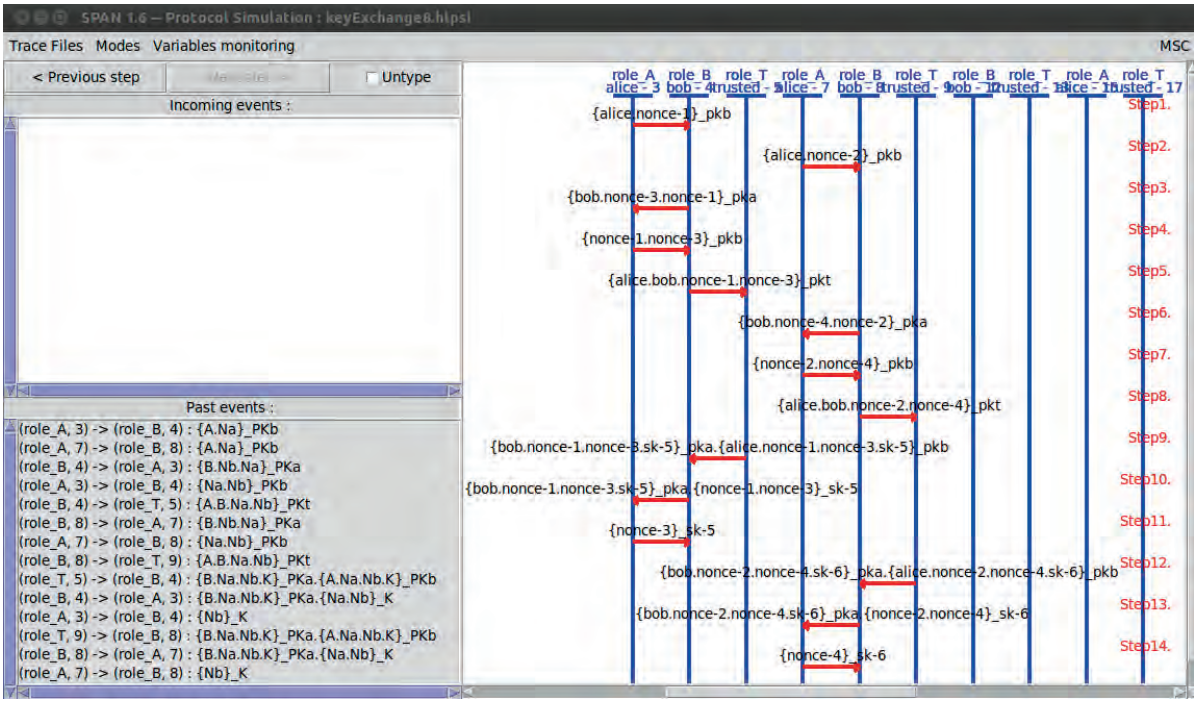

Рис. 6. Эмуляция протокола безопасности на AVISPA

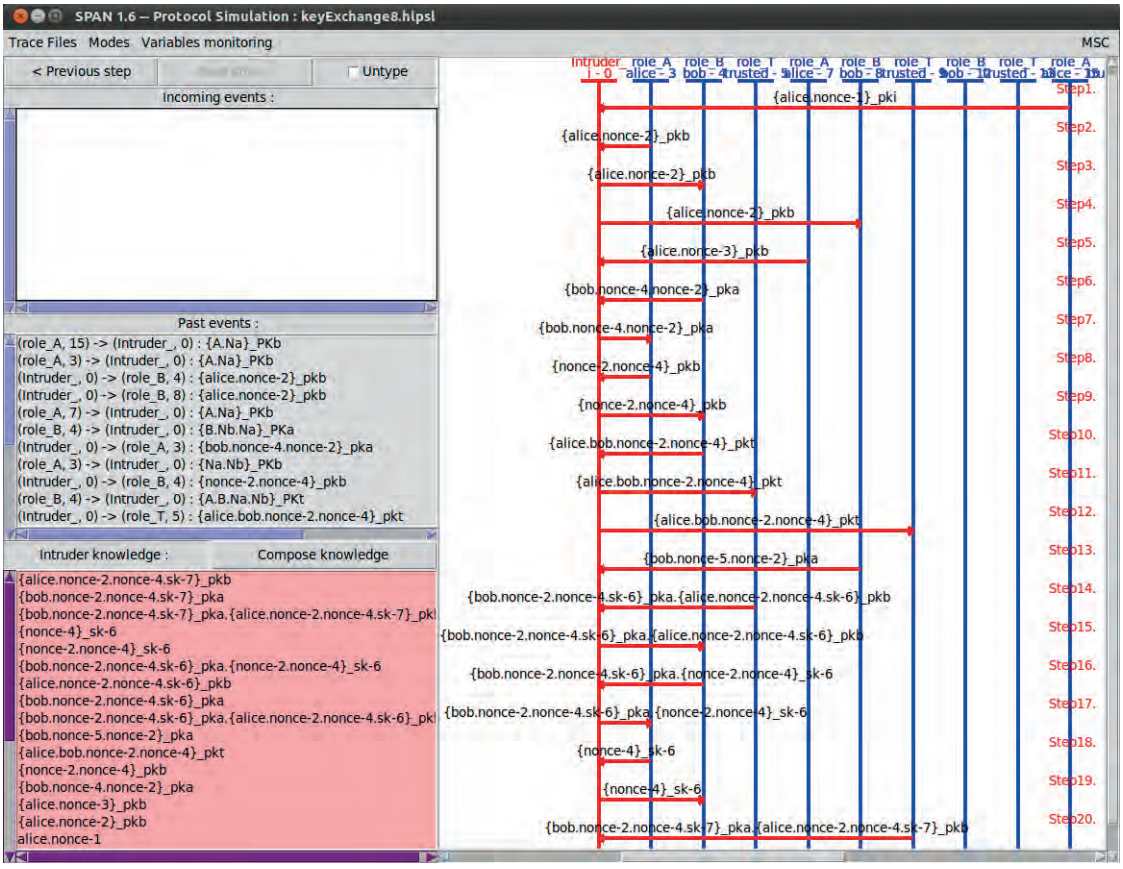

Рис. 7. Эмуляция протокола с учётом действий злоумышленника

ных условиях функционирования с использованием специализированного инструментального средства. Результаты моделирования подтверждают информационную безопасность предложенного протокола по обеспечению взаимной аутентификации, конфиденциальности данных, предотвращению атак MITM и повтора в рамках заданных ограничений.

Применение предлагаемых решений целесообразно для решения задач обеспечения конфиденциальности частной информации в системе отслеживания на основе блокчейна. В частности – для решения задач обеспечения аутентифицированного доступа к приватной части записи блока распределённого реестра, что является типовой задачей в системах прослеживаемости качества товара.

Литература

1. Петренко А. С., Петренко С. А. Метод оценивания квантовой устойчивости блокчейн-платформ //Вопросы кибербезопасности. – 2022. – №. 3 (49). – С. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22
2. Комарова А. В., Коробейников А. Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи //Вопросы кибербезопасности. – 2019. – №. 2 (30). – С. 58-68. DOI: 10.21681/2311-3456-2019-2-58-68
3. Макаров В. В., Волчик О. В. Цифровизация систем менеджмента качества в нефтегазовой отрасли // Экономика и качество систем связи. – 2023. – №. 1 (27). – С. 4–13.
4. Kolesnikova D. et al. Features of information support for decision-making in planning production processes //AIP Conference Proceedings. – AIP Publishing LLC, 2021. – Т. 2402. – №. 1. – С. 040036. DOI: 10.1063/5.0071707
5. Usova M., Chuprov S., Viksnin I. Informational space and messages interaction models for smart factory concept //2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. – IEEE, 2020. – С. 617–621. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138292
6. 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
7. Котенко И.В., Саенко И.Б., Захарченко Р.И., Капустин А.С., Аль-Барри М.Х., Управление доступом к электронной информационно-образовательной среде вузов федеральных органов исполнительной власти// Вопросы кибербезопасности. 2023. № 2 (54). С. 73-84. DOI: 10.21681/2311-3456-2023-2-73-84
8. Куликов А. Л., Зинин В. М. Требования к информационной безопасности в электроэнергетике и их реализация в интеллектуальных устройствах цифровых подстанций //Интеллектуальная электротехника. – 2022. – №. 3 (19). – С. 49–78. DOI 10.46960/2658-6754_2022_3_49
9. Болдырев И. А. и др. Концепция распределённой ИИУС на основе технологий промышленного IoT для повышения отслеживаемости, экономичности и безопасности систем микрогрид //Современные проблемы теплофизики и энергетики. – 2020. – С. 489–490.
10. Язов Ю. К., Авсентьев А. О. Пути построения многоагентной системы защиты информации от утечки по техническим каналам // Вопросы кибербезопасности. – 2022. – №. 5. – С. 51. DOI: 10.21681/2311-3456-2022-5-2-13
11. Viksnin I. I., Marinenkov E. D., Chuprov S. S. A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms //Научно-технический вестник информационных технологий, механики и оптики. – 2022. – Т. 22. – №. 1. – С. 47-59. DOI: 10.17586/2226-1494-2022-22-1-47-59
12. Балюк А. А., Финько О. А. Многоагентная аутентификация цифровых двойников в киберфизических системах //Вопросы кибербезопасности. – 2022. – №. 5. – С. 51. DOI: 10.21681/2311-3456-2022-5-100-113
13. Yingwen Chen, Linghang Meng, Huan Zhou, Guangtao Xue, «A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection», Wireless Communications and Mobile Computing, vol. 2021, Article ID 6685762, 12 pages, 2021. https://doi.org/10.1155/2021/6685762
14. Zheng BK, Zhu LH, Shen M et al. Scalable and privacy-preserving data sharing based on blockchain. Journal of computer science and technology 33(3): 557–567 May 2018. DOI 10.1007/s11390-018-1840-5
15. Yuhan Yang, Lijun Wei, Jing Wu, and Chengnian Long. 2020. Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20). Association for Computing Machinery, New York, NY, USA, March 2020 Pages 46–51. https://doi.org/10.1145/3390566.3391664
16. Миронов А. М. Математическая модель и методы верификации криптографических протоколов //Интеллектуальные системы. – 2022. – Т. 26. – №. 2. – С. 85–144.
17. Нестеренко А. Ю., Семенов А. М. Методика оценки свойств безопасности криптографических протоколов //Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В. Арменского. – 2021. – С. 249–251.
18. Перевышина Е. А., Бабенко Л. К. Моделирование свойств безопасности аутентификации криптографических протоколов с использованием средств формальной верификации SPIN //Информатизация и связь. – 2020. – №. 3. – С. 21-25. DOI: 10.34219/2078-8320-2020-11-3-21-25
19. Михайлова А. А., Уманский С. А., Шустрова А. Н. Критерии и методы оценки безопасности протоколов аутентификации //Цифровая наука. – 2021. – №. 6–1. – С. 4–10.

VERIFICATION OF SESSION KEY SAFE DISTRIBUTION METHOD IN THE PRODUCT QUALITY TRACEABILITY SYSTEM

Le W.H.[8], Begaev A.N.[9], Komarov I.I.[10], Fung W.K.[11]

The purpose of the work is *to determine the requirements for ensuring the basic and additional properties of information security in the interaction of counterparties in information systems related to ensuring the traceability of product quality; to develop and formally verify the method of generation and secure distribution of a session key that meets these requirements.*

Result: *The use of product quality traceability systems is a powerful tool for solving a wide range of technological and social problems, for example: state control in regulated areas, ensuring consumer safety, forming a competitive advantage of the manufacturer, etc. However, the widespread introduction of such decentralized systems is associated with a number of contradictions, one of which is directly related to the problem of ensuring data confidentiality and the need for their controlled use in the dynamic composition of counterparties and consumers. The paper proposes a direction for overcoming this contradiction by forming scenarios for obtaining controlled access to the private information of the interacting party using cryptographic procedures. To implement such scenarios, a method and a protocol based on it have been developed for generating and distributing a secret session key using a trusted third party. A formal proof of the security of the proposed solution is provided using a specialized tool for protocol verification. The results obtained are primarily focused on application in distributed ledger systems, which involve the division of data into private and public blocks. However, they can also be used in other systems that require confidentiality, accessibility, and unprovability, especially when there are limitations on computing resources.*

Scientific novelty: *consists in the problem-oriented analysis of the specific requirements for ensuring the information security of the process of entering and extracting data into the system for tracking the quality of goods in the given scenarios of its use. Based on the selected requirements, the problem of developing an adapted method for generating and distributing a secret session key between two subscribers with the involvement of a trusted party is formulated and solved. Based on the developed A practical communication protocol is synthesized and a formal proof of compliance with the specified information security requirements, resistance to MITM and repetition attacks is carried out.*

Keywords: *cybersecurity, confidentiality, non-repudiation, session cryptographic key, distributed register, formal protocol verification.*

References

1. Petrenko A. S., Petrenko S. A. Metod ocenivanija kvantovoj ustojchivosti blokchejn-platform //Voprosy kiberbezopasnosti. – 2022. – №. 3 (49). – S. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22
2. Komarova A. V., Korobejnikov A. G. Analiz osnovnyh sushhestvujushhih post-kvantovyh podhodov i shem jelektronnoj podpisi //Voprosy kiberbezopasnosti. – 2019. – №. 2 (30). – S. 58-68. DOI: 10.21681/2311-3456-2019-2-58-68
3. Makarov V. V., Volchik O. V. Cifrovizacija sistem menedzhmenta kachestva v neftegazovoj otrasli // Jekonomika i kachestvo sistem svjazi. – 2023. – №. 1 (27). – S. 4–13.
4. Kolesnikova D. et al. Features of information support for decision-making in planning production processes //AIP Conference Proceedings. – AIP Publishing LLC, 2021. – T. 2402. – №. 1. – S. 040036. DOI: 10.1063/5.0071707
5. Usova M., Chuprov S., Viksnin I. Informational space and messages interaction models for smart factory concept //2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. – IEEE, 2020. – S. 617–621. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138292

8 Le W.H., Ph.D. student, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: hieule250715@gmail.com

9 Alexey N. Begaev, Ph.D. (Technology), Professor at ITMO University, CEO of Echelon North-West, St. Petersburg, Russia. E-mail: begaev@mail.ru

10 Igor I. Komarov, Ph.D. (Physics & Mathematics), Associate Professor, Faculty of Information Technology Security, ITMO University, St. Petersburg, Russia. E-mail: i_krov@mail.ru

11 Fung W.K., Ph.D. student, Faculty of Software Engineering and Computer Engineering, ITMO University, St. Petersburg, Russia. E-mail: hieule250715@gmail.com

6. Lje V., Vu L., Komarov I. I. Obespechenie informacionnoj bezopasnosti v sisteme proslezhivaemosti moreproduktov na osnove tehnologii blokchejna // Nauka i biznes: puti razvitija - 2022. - № 5(131). - S. 97–101
7. Kotenko I.V., Saenko I.B., Zaharchenko R.I., Kapustin A.S., Al'-Barri M.H., Upravlenie dostupom k jelektronnoj informacionno-obrazovatel'noj srede vuzov federal'nyh organov ispolnitel'noj vlasti//Voprosy kiberbezopasnosti. 2023. № 2 (54). S. 73-84. DOI: 10.21681/2311-3456-2023-2-73-84
8. Kulikov A. L., Zinin V. M. Trebovanija k informacionnoj bezopasnosti v jelektrojenergetike i ih realizacija v intellektual'nyh ustrojstvah cifrovyh podstancij //Intellektual'naja jelektrotehnika. – 2022. – №. 3 (19). – S. 49–78. DOI 10.46960/2658-6754_2022_3_49
9. Boldyrev I. A. i dr. Koncepcija raspredeljonnoj IIUS na osnove tehnologij promyshlennogo IoT dlja povyshenija otslezhivaemosti, jekonomichnosti i bezopasnosti sistem mikrogrid //Sovremennye problemy teplofiziki i jenergetiki. – 2020. – S. 489–490.
10. Jazov Ju. K., Avsent'ev A. O. Puti postroenija mnogoagentnoj sistemy zashhity informacii ot utechki po tehnicheskim kanalam //Voprosy kiberbezopasnosti. – 2022. – №. 5. – S. 51. DOI: 10.21681/2311-3456-2022-5-2-13
11. Viksnin I. I., Marinenkov E. D., Chuprov S. S. A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms //Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. – 2022. – T. 22. – №. 1. – S. 47-59. DOI: 10.17586/2226-1494-2022-22-1-47-59
12. Baljuk A. A., Fin'ko O. A. Mnogoagentnaja autentifikacija cifrovyh dvojnikov v kiberfizicheskih sistemah //Voprosy kiberbezopasnosti. – 2022. – №. 5. – S. 51. DOI: 10.21681/2311-3456-2022-5-100-113
13. Yingwen Chen, Linghang Meng, Huan Zhou, Guangtao Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6685762, 12 pages, 2021. https://doi.org/10.1155/2021/6685762
14. Zheng BK, Zhu LH, Shen M et al. Scalable and privacy-preserving data sharing based on blockchain. Journal of computer science and technology 33(3): 557–567 May 2018. DOI 10.1007/s11390-018-1840-5
15. Yuhan Yang, Lijun Wei, Jing Wu, and Chengnian Long. 2020. Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20). Association for Computing Machinery, New York, NY, USA, March 2020 Pages 46–51. https://doi.org/10.1145/3390566.3391664
16. Mironov A. M. Matematicheskaja model' i metody verifikacii kriptograficheskih protokolov //Intellektual'nye sistemy. – 2022. – T. 26. – №. 2. – S. 85–144.
17. Nesterenko A. Ju., Semenov A. M. Metodika ocenki svojstv bezopasnosti kriptograficheskih protokolov //Mezhvuzovskaja nauchno-tehnicheskaja konferencija studentov, aspirantov i molodyh specialistov imeni E.V. Armenskogo. – 2021. – S. 249–251.
18. Perevyshina E. A., Babenko L. K. Modelirovanie svojstv bezopasnosti autentifikacii kriptograficheskih protokolov s ispol'zovaniem sredstv formal'noj verifikacii SPIN //Informatizacija i svjaz'. – 2020. – №. 3. – S. 21-25. DOI: 10.34219/2078-8320-2020-11-3-21-25
19. Mihajlova A. A., Umanskij S. A., Shustrova A. N. Kriterii i metody ocenki bezopasnosti protokolov autentifikacii //Cifrovaja nauka. – 2021. – №. 6–1. – S. 4–10.