ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ
(ВАК – 05.13.00)
7. 2021 (ИЮНЬ)

ВЕСТНИК
СОВРЕМЕННЫХ
ЦИФРОВЫХ
ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

www.c3da.org

№7
ИЮНЬ 2021

ISSN 2686-9373

Издатель: *Ассоциация специалистов в области развития криптовалют и цифровых финансовых активов*
Центр развития криптовалют и цифровых финансовых активов
Адрес редакции и издателя: 125315, Москва, Усиевича, 20, каб. 207
Тел/факс: *8 (499) 155-43-26*
E-mail: accda@c3da.org
info@c3da.org

Подписано в печать 25.06.2021 г.

Тираж 500 экз.

Подписной индекс в каталоге «Пресса России»: 79111

Свидетельство о регистрации СМИ
ПИ № ФС 77-76187 от 08.07.2019 г.

РЕДАКЦИОННЫЙ СОВЕТ

АССОЦИАЦИЯ РКЦФА

Ассоциация специалистов
в области развития криптовалют
и цифровых финансовых активов

Центр развития криптовалют
и цифровых финансовых активов

Мы не предсказываем цифровое будущее.
Мы его создаём!

c3da.org
accda@c3da.org
info@c3da.org

**Единственная в России научная организация,
занимающаяся фундаментальными и прикладными аспектами
современных цифровых технологий, в первую очередь -
распределенными реестрами
и цифровыми активами.**

**В нашем портфолио - целый ряд
уникальных успешных проектов
в области разработки и сертификации распределенных реестров,
цифровых платформ и токенов, высокозащищеных систем
технической и финансовой прогностики и мониторинга,
а также семантического искусственного интеллекта.**

Ассоциация РКЦФА - объединение ведущих российских специалистов в области цифровых технологий.

Мы ведём
авторские обучающие программы и курсы
в области цифровых технологий и криптографии
для технологических лидеров России.

СОДЕРЖАНИЕ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Седьмой номер «Вестника современных цифровых технологий» выходит на фоне знаменательного события – 100-летия криптографической службы Российской Федерации. Созданная в динамичные годы революции и гражданской войны и впитавшая всю славную историю нашей страны, криптографическая служба России эволюционировала до крупнейшей и сильнейшей в мире специальной службы, сотрудников которой счел возможным отдельно поздравить 5 мая Президент Российской Федерации. Сегодня не теряют своей актуальности вопросы развития современных методов криптографической защиты информации, от решения которых зависит уровень обеспечения безопасности страны и способность противостоять современным угрозам и вызовам, таким как кибертерроризм.

Мы с радостью отмечаем, что эта важнейшая для нашего журнала дата совпадает с включением в состав редакционного совета Георгия Сергеевича Елизарова, доктора технических наук, академика Академии криптографии РФ, директора НИИ «Квант» – ведущего предприятия в области защиты информации, в том числе и криптографическими методами. Георгий Сергеевич высоко оценил усилия нашего журнала в области информационной безопасности.

Поистине замечательно и то, что в состав нашего редакционного совета вошел доктор физико-математических наук, профессор, академик РАН Александр Сергеевич Сигов, лауреат Государственной премии РФ, премии Правительства РФ в области образования и двух премий Правительства РФ в области науки и техники, президент МИРЭА, ученый с мировым именем и заслуженный деятель науки Российской Федерации, член Научного совета при Совете Безопасности РФ.

В седьмом номере нашего журнала большое внимание уделено фундаментальным аспектам цифровых технологий. В разделе «ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ» представлены следующие материалы.

В статье **«Современное состояние методологии построения защищенной квантовой сети»** коллектива авторов рассматриваются актуальные вопросы организации квантово-защищенных сетей для обеспечения безопасного распределения ключей между удаленными абонентами и СКЗИ, представлен подход к организации квантовых сетей, позволяющий формировать квантово-защищенный ключ между опорными узлами сети, описана структура подсистемы организации доверенных промежуточных узлов.

Детальный анализ современного состояния новой научной области – систем конфиденциального и проверяемого машинного обучения – представлен в статье **«Конфиденциальное машинное обучение с нулевым разглашением»**. Авторами описывается система доказательства с нулевым разглашением универсального назначения, рассматриваются основные идеи, заложенные в основу существующих реализаций систем конфиденциального и проверяемого машинного обучения.

В работе **«Обоснование свойств цифровых платформ в рамках субъектно-объектной модели компьютерных систем»** рассматриваются основные понятия и свойства цифровых платформ с позиций теоретической субъектно-объектной модели компьютерных систем. Приводится обоснование взаимосвязи свойств потоков и процессов порождений субъектов компьютерной системы со свойствами интегрируемости и развития цифровых платформ.

Раздел «ЭКОНОМИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ» включает интересную статью коллектива авторов **«Методология создания прототипа универсальной цифровой монеты»**. Цифровая монета рассматривается как средство достижения независимости и мобильности национальной финансовой системы, снижения издержек на бумажное денежное обращение, укрепления экономической безопасности государства. Приводится предварительная структура цифровой монеты и краткое описание системы и технологии обращения цифровых монет.

Интересно отметить, что, казалось бы, чисто экономическая и политическая проблема универсальной монеты как средства платежа, поддерживающего трансграничные операции, целиком базируется на криптографических алгоритмах.

В разделе «ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОМЫШЛЕННОСТИ» представлена статья **«Концепция информационной безопасности «роя» киберфизических систем»**, посвященная рассмотрению возможных подходов к обеспечению информационной безопасности киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра». В статье предложено решение данных вопросов при помощи включения функций формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности, в киберфизических устройствах. Описан алгоритм обеспечения информационной безопасности «роя» киберфизических устройств.

Раздел «ЛИТЕРАТУРА О ЦИФРОВЫХ ТЕХНОЛОГИЯХ» завершает седьмой выпуск. В нем представлен рассказ нашего традиционного автора Егора Федорова **«Яви мне чудо»**. Развивая идеи С. Панова о «цифровой духовности» автор пытается понять, что могло бы стать началом создания новой духовной традиции в цифровом мире?

УДК: 004.75, 004.41

Современное состояние методологии построения защищенной квантовой сети

E.V. Vereshchagina, V.I. Egorov, A.A. Santev, S.E. Khoruzhnikov, A.Yu. Shcherbakov

The Current State of the Methodology for Constructing a Secure Quantum Network

Abstract. *The article is devoted to the topical problem of the organization of quantum-protected networks to ensure secure distribution of keys between remote subscribers and CIPF (cryptographic information protection facility). An approach to the organization of quantum networks based on trusted intermediate backbone nodes is considered, which makes it possible to form a quantum-protected key between the backbone network nodes based on quantum keys. The structure of the subsystem for organizing trusted intermediate nodes is described.*

Keywords: *quantum cryptographic system for generating and distributing keys, quantum key distribution, quantum key, quantum protected key, means of cryptographic information protection.*

Е.В.Верещагина[1]
В.И.Егоров[2]
А.А. Сантьев[3]
С.Э.Хоружников[4]
А.Ю.Щербаков[5]
[1]Генеральный директор ООО «Смартс-Квантителеком».
E-mail: vereschagina@qcphotonics.com
[2]Доцент, кандидат физико-математических наук,технический директор лидирующего исследовательского центра «Национальный центр квантового интернета», Национальный исследовательский университет ИТМО.
E-mail: viegorov@itmo.ru
[3]Сотрудник лидирующего исследовательского центра «Национальный центр квантового интернета», Национальный исследовательский университет ИТМО.
E-mail: aasantev@itmo.ru
[4]Доцент, кандидат физико-математических наук, директор лидирующего исследовательского центра «Национальный центр квантового интернета», Национальный исследовательский университет ИТМО
E-mail: xse@itmo.ru
[5]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена актуальной проблеме организации квантово-защищенных сетей для обеспечения безопасного распределения ключей между удаленными абонентами и СКЗИ. Рассматривается подход к организации квантовых сетей на основе доверенных промежуточных опорных узлов, позволяющий формировать квантово-защищенный ключ между опорными узлами сети на основе квантовых ключей. Описывается структура подсистемы организации доверенных промежуточных узлов.*

Ключевые слова: *квантовая криптографическая система выработки и распределения ключей, квантовое распределение ключей, квантовый ключ, квантово-защищенный ключ, средство криптографической защиты информации.*

ВВЕДЕНИЕ. СЕРВИСНАЯ МОДЕЛЬ КВАНТОВОЙ СЕТИ

Технология квантового распределения криптографических ключей решает одну из основных задач криптографии - гарантированное на уровне физических законов защищенное распределение ключей между удаленными абонентами и средствами криптографической защиты информации (СКЗИ) [1]. Данная технология является одним из основных направлений развития прикладной квантовой криптографии [2].

Квантовая криптографическая система выработки и распределения ключей (ККС ВРК) представляет собой совокупность программно-аппаратных криптографических средств, реализующих квантовый криптографический протокол выработки и распределения ключей для территориально-распределенных СКЗИ.

Предположим, что ККС ВРК состоит из двух территориально удаленных друг от друга модулей ККС ВРК А и ККС ВРК Б. Квантовая аппаратура обеспечивает взаимодействие по квантовому каналу, причем ККС ВРК А реализует передачу кодированных квантовых состояний, а ККС ВРК Б – детектирование квантовых состояний, поэтому ККС ВРК А также может также

именоваться отправителем, а ККС ВРК Б – получателем. Один из возможных способов реализации ККС ВРК заключается в использовании фазового кодирования, реализованного на боковых частотах модулированного излучения [3].

Важно заметить, что ККС ВРК функционирует в рамках сервисной модели [4], в которой определены следующие уровни:

– первый уровень сервисной модели (СМ): получение ключей от устройств КРК с одновременным мониторингом их количества и параметров;

– второй уровень: хранение квантовых ключей с их учетом и маркировкой;

– третий уровень: передача квантовых ключей потребителям по установленным протоколам и интерфейсам;

– четвертый уровень: использование ключей конечными потребителями.

Предлагается рассмотреть и сравнить три типа защищенных сетей и четыре параметра, описывающие свойства системы распределения ключей:

– **сеть типа 1**: сеть с предварительно распределенными ключами.

– **сеть типа 2**: сеть с выработкой и распределением ключей при помощи датчиков случайных чисел (ДСЧ);

– **сеть типа 3**: квантовая сеть, у которой между соседними узлами генерируются одинаковые квантовые ключи.

Для каждого типа сетей вводится четыре параметра:

– необходимость предварительной доставки ключей на узлы сети;

– трудоемкость распределения ключей по узлам сети;

– время актуального действия ключа;

– трудоемкость замены ключа при компрометации.

Тогда сравнение различных типов сетей по указанным параметрам можно представить в таблице 1.

Таблица 1

Сравнение типов защищенных сетей (по параметру распределения ключей)

Тип сети, параметры	Сеть 1-го типа («классическая»)	Сеть 2-го типа (усиленная ДСЧ)	Сеть 3-го типа («квантовая»)
Необходимость предварительной доставки ключей на узлы сети	Да	Да	Нет
Трудоемкость распределения ключей по узлам сети	Высокая	Средняя	Минимальная
Время актуального действия ключа	Определено формуляром СКЗИ	Определено формуляром СКЗИ	Не ограничено
Трудоемкость замены ключа при компрометации	Высокая (новое распределение ключей)	Средняя (определена запасом предварительно выработанной матрицы)	Минимальная (автоматическая смена)

Таким образом, сеть третьего типа, то есть квантовая сеть, обладает выраженными преимуществами по сравнению с другими типами.

СПОСОБЫ ФОРМИРОВАНИЯ КВАНТОВО-ЗАЩИЩЕННОГО КЛЮЧА В КВАНТОВОЙ СЕТИ

Поскольку ККС ВРК состоят из двух модулей:

ККС ВРК А и ККС ВРК Б, они способны обеспечивать квантовыми ключами только те узлы сети, в которых непосредственно расположены модули. При этом дальность рассылки квантового ключа также ограничена из-за затухания оптических сигналов при их распространении в оптическом волокне. Кроме того, из-за лежащих в основе ККС ВРК физических принципов обеспечения защищенного распределения ключей между удаленными абонентами и СКЗИ для увеличения дальности рассылки квантовых ключей не представляется возможным использовать классические телекоммуникационные волоконные усилители или повторители. Квантовые повторители могут быть разработаны на основе устройств квантовой памяти и являются перспективным решением проблемы организации квантовых сетей, однако деятельность по их разработке в настоящее время находится на стадии научных исследований [5].

Из-за ограниченности топологии точка-точка возникает необходимость увеличивать дальность выработки квантовых ключей. Кроме того, для масштабирования технологии КРК также необходимо реализовывать многопользовательские квантовые сети, но топология точка-точка также накладывает ограничения на возможности по построению многопользовательских сетей. Возникает проблема интеграции ККС ВРК в платформенные решения цифровых технологий, использующих криптографические механизмы при обеспечении собственной функциональности [6].

В настоящее время для преодоления накладываемых ограничений широко используется подход к организации квантовых сетей на основе доверенных промежуточных опорных узлов (ПОУ), позволяющий формировать квантово-защищенный ключ (КЗК) между опорными узлами сети (ОУ) на основе квантовых ключей (КК). Наиболее распространенными являются два подхода к формированию КЗК. Первый подход заключается в использовании операции сложения по модулю два (исключающее ИЛИ - XOR), применяемой к выработанным между соседними узлами КК. Второй подход основан на формировании КЗК в виде некоторой исходной последовательности, которая впоследствии передается от одного ОУ к другому ОУ через цепочку ПОУ с перешифрованием на квантовых ключах в каждом узле.

Рассмотрим подробнее первый подход (использование операции XOR) на основе квантовой сети простейшей топологии, когда один ПОУ соединяет две разнесенные линии квантовой коммуникации (Рис. 1).

В такой конфигурации ПОУ состоит из двух модулей КРК. В ПОУ, после осуществления сеансов КРК между каждым из ОУ и ПОУ, формируются два отдельных секретных квантовых ключа $КК_1$ и $КК_2$. По окончании сеансов распределения ключей, в промежуточном опорном узле осуществляется операция сложения по модулю два (операции XOR) над сгенерированными секретными ключами $КК_1$ и $КК_2$:

$$К_{1,2}=КК_1 \oplus КК_2.$$

Результат операции сложения по модулю два $К_{1,2}$ объявляется ПОУ по открытому кана-

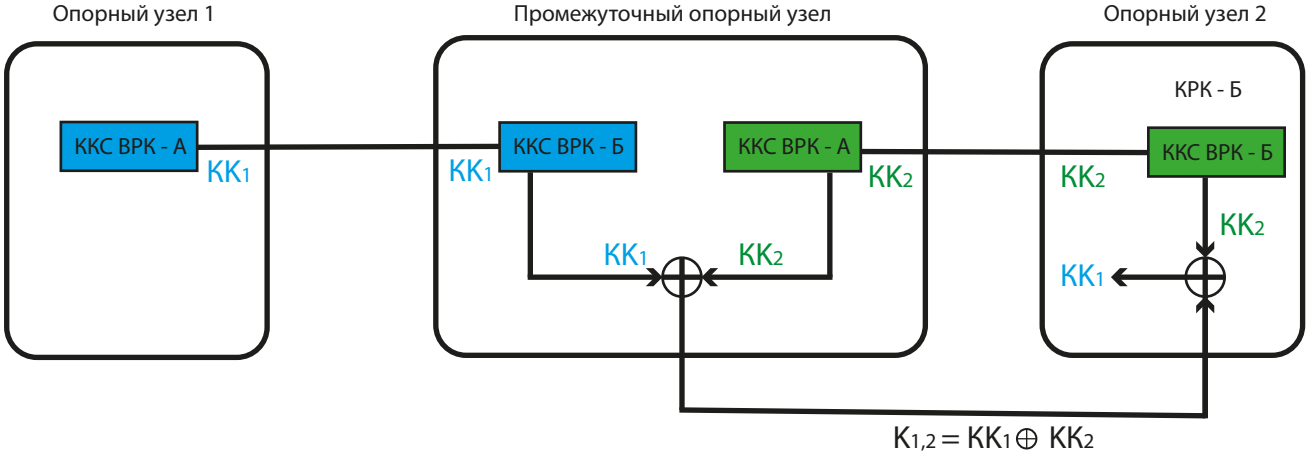

Рис. 1. Упрощенная схема квантовой сети с двумя опорными узлами и одним промежуточным опорным узлом, в которой выработка КЗК осуществляется с использованием операции XOR

лу связи. Знание непосредственно результата операции сложения по модулю два $К_{1,2}$ не дает злоумышленнику никакой информации о $КК_1$ и $КК_2$. Однако, поскольку в ПОУ происходит обмен классической информацией между двумя модулями КРК, подключенными к различным линиям квантовой коммуникации, возможность доступа злоумышленника к данному узлу должна быть исключена. В дальнейшем одним из опорных узлов осуществляется еще одна операция сложения по модулю два, только уже над объявленной промежуточным опорным узлом битовой последовательностью $К_{1,2}$ и известным ему КК. Осуществляющей данную операцию стороне удается восстановить КК, сгенерированный на другой линии квантовой коммуникации. В случае, когда данную операцию выполняет $ОУ_2$, она может быть записана следующим образом:

$КК_1^{(ОУ2)} = К_{1,2} \oplus КК_2 = КК_1$.

Таким образом удается доставить $КК_1$ во $ОУ_2$, после чего $КК_1$ становится известен обоим узлам и может использоваться для шифрования и расшифрования данных. Поскольку фактически данный подход подразумевает передачу $КК_1$ классическими методами с его шифрованием и расшифрованием при использовании $КК_2$, то после осуществления данной процедуры он является квантово-защищенным ключом. Следует отметить, что при использовании данного подхода аналогичную процедуру можно реализовать и для $КК_2$, зная $К_{1,2}$.

Другой возможный вариант по выработке КЗК заключается в передаче заранее сформированного КЗК от $ОУ_1$ к $ОУ_2$ в зашифрованном виде, с использованием КК. В таком случае ключевая последовательность КЗК, сгенерированная в $ОУ_1$, будет последовательно в зашифрованном виде передаваться между узлами, имеющими общую линию квантовой коммуникации. При этом в каждом из ПОУ передаваемое сообщение будет перешифровываться. В таком случае исходная ключевая последовательность также будет являться КЗК, поскольку ее передача между опорными узлами осуществляется в защищенном виде, с использованием КК. Рассмотрим данный принцип выработки КЗК на примере квантовой сети, состоящей из двух ОУ и одного ПОУ. Сначала в $ОУ_1$ осуществляется шифрование КЗК с использованием $КК_1$, после чего он в зашифрованном виде отправляется в ПОУ. В ПОУ происходит расшифрование полученного в зашифрованном виде КЗК с использованием $КК_1$. этого КЗК снова шифруется, однако в этот раз шифрование осуществляется с использованием $КК_2$. Далее КЗК в зашифрованном виде передается в $ОУ_2$, где происходит расшифрование полученного в зашифрованном виде КЗК с использованием $КК_2$. Упрощенная схема квантовой сети, использующей данный принцип доставки КЗК, представлена на рисунке 2.

ПОДСИСТЕМА ОРГАНИЗАЦИИ ДОВЕРЕННЫХ ПРОМЕЖУТОЧНЫХ УЗЛОВ

При организации квантовых сетей с доверенными ПОУ необходимо формирование КЗК, требующее разработки и использования дополнительного программно-аппаратного обеспечения, а именно – подсистемы организации доверенных промежуточных узлов (в литературе и технической документации применяется

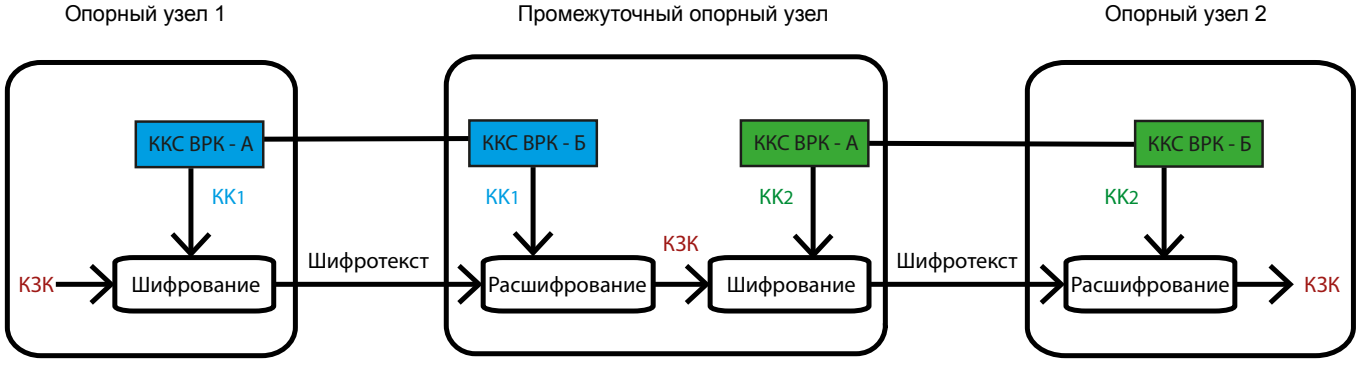

Рис. 2. Упрощенная схема магистральной квантовой сети с двумя опорными узлами и одним промежуточным доверенным узлом

также эквивалентный термин «промежуточный доверенный узел» (ПДУ)). В общем случае ПДУ представляет собой устройство, объединяющее в едином конструктивном исполнении подсистему шифрования ПДУ (ПШ ПДУ) и сервер ПДУ, на который устанавливается сетевая ПДУ (СПДУ), программное обеспечение высокого уровня.

Основное назначение ПДУ заключается в выполнении функций, связанных с формированием КЗК. Таким образом, ПДУ должна реализовывать один из ранее рассмотренных способов формирования КЗК. При выборе подхода к формированию КЗК, заключающегося в передаче заранее сформированного КЗК между ОУ в зашифрованном с помощью различных КК виде, ПДУ должна осуществлять перешифрование КЗК в каждом из узлов с использованием КК, получаемых ею от модулей ККС ВРК, расположенных в одном с ПДУ узле. Из этого следует, что ПДУ и ККС ВРК должны иметь интерфейс для передачи КК. После формирования КЗК ПДУ также должны обеспечивать выдачу КЗК СКЗИ, расположенным в узле. Как правило СКЗИ для обеспечения защищенной передачи пользовательских данных располагаются только в ОУ или ОКУ, а в ПОУ не используются. Таким образом, ПДУ также должна иметь интерфейсы для выдачи КЗК в СКЗИ, и также сами СКЗИ должны быть подготовлены для работы с ПДУ.

Кроме того, целесообразно передать ПДУ часть иных функций, необходимых для обеспечения функционирования ККС ВРК. В частности, целесообразно реализовывать передачу служебного канала ККС ВРК, необходимого для реализации протокола квантовой рассылки ключей, посредством ПДУ, поскольку при передаче служебного канала ККС ВРК необходимо обеспечивать его имитозащиту. Также ПДУ должна осуществлять функции, связанные с хранением криптографических ключей в памяти с учетом всех специальных требований и управлением жизненным циклом ключей, а также выработкой случайных чисел для модулей ККС ВРК с использованием встроенного генератора случайных чисел. При реализации системы управления и мониторинга квантовой сети, на ПДУ также могут быть возложены функции по передаче команд управления к модулям ККС ВРК, а также получению и обработке информации мониторинга от модулей ККС ВРК. Таким образом, при построении квантовой сети ПДУ также будет взаимодействовать с расположенными в каждом из узлов программно-аппаратными компонентами подсистемы управления и мониторинга, при этом позволяя осуществлять управление и мониторинг как самой ПДУ, так и модулями ККС ВРК. Схематично работа ПДУ представлена на рисунке 3.

СРАВНЕНИЕ СПОСОБОВ ОРГАНИЗАЦИИ КВАНТОВОЙ СЕТИ НА ОСНОВЕ ДОВЕРЕННЫХ ПОУ

В общем случае есть два способа организации квантовых сетей на основе доверенных ПОУ: с перешифрованием данных в каждом узле на квантовых ключах и с формированием

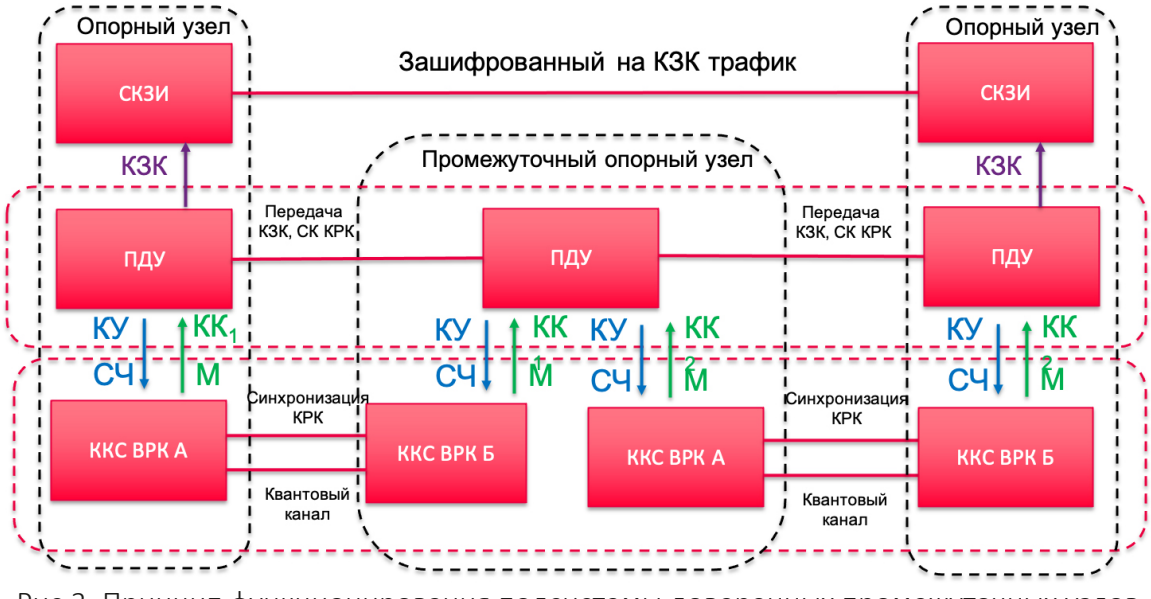

Рис.3. Принцип функционирования подсистемы доверенных промежуточных узлов

квантово-защищенных ключей и шифрованием данных в опорных узлах. Рисунки с подходами.

Можно выделить два способа организации квантово-защищенной передачи данных между ОУ:

– использование КК для шифрования данных, с применением расположенных в каждом узле СКЗИ;

– использование КЗК для шифрования данных, с применением расположенных в опорных узлах СКЗИ. Указанные способы проиллюстрированы на рисунках 4а и 4б.

Подход, связанный с применением КК для шифрования данных и размещением СКЗИ в каждом узле, предполагает использование для передачи данных между СКЗИ квантовых ключей, вырабатываемых на каждом участке квантовой сети. При этом последние расположены в тех же узлах, что и модули КРК, с использованием которых вырабатывался используемый для шифрования данных КК. В таком случае для обеспечения квантово-защищенной передачи данных между ОУ выполняется последовательная передача зашифрованных данных через все пары промежуточных опорных узлов. Перешифрование данных осуществляется в каждом ПОУ.

При использовании КЗК для шифрова-

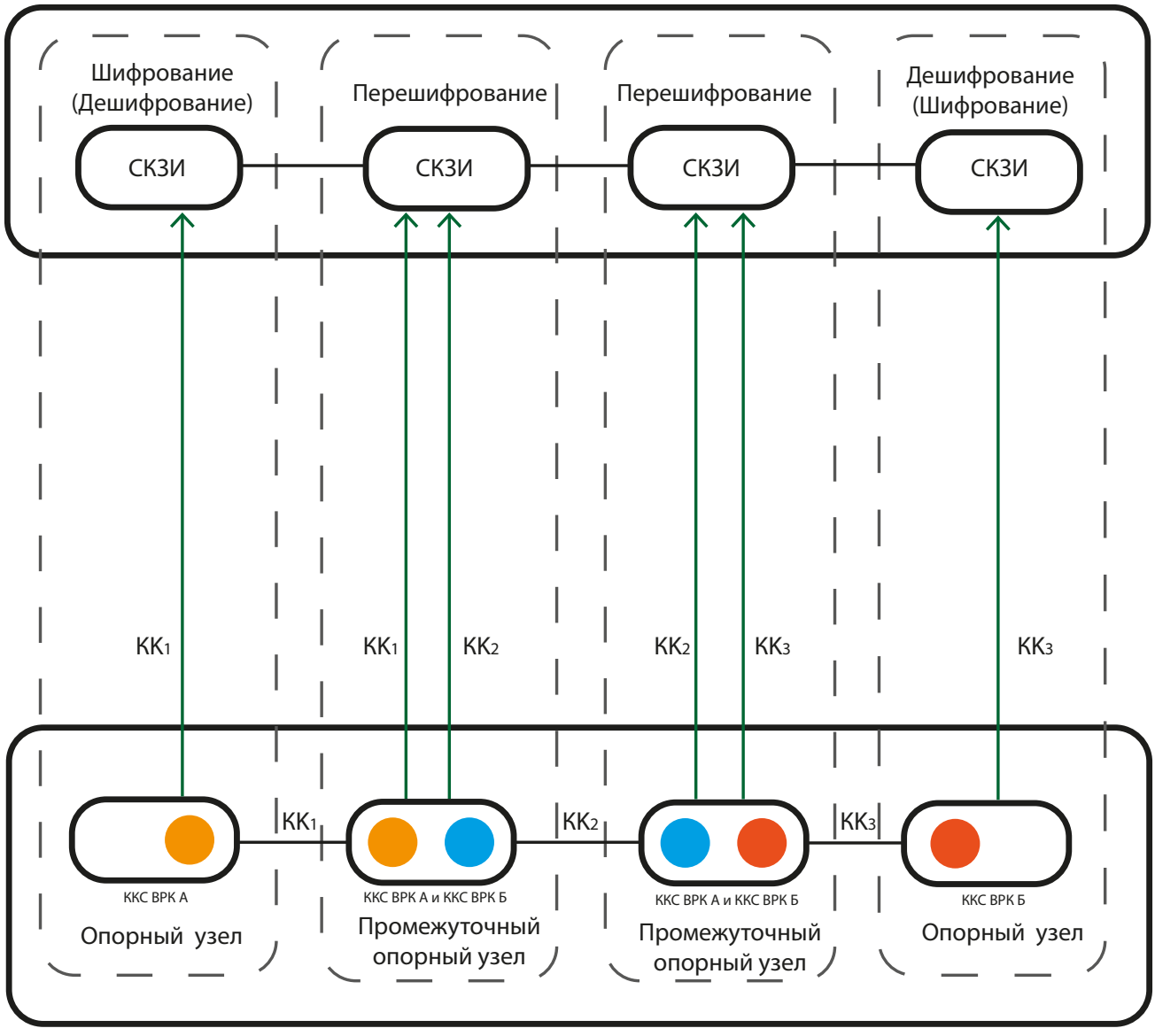

Рис. 4а. Способ организации квантово-защищенной передачи данных, основанный на использовании КК для шифрования данных, с применением расположенных в каждом узле СКЗИ

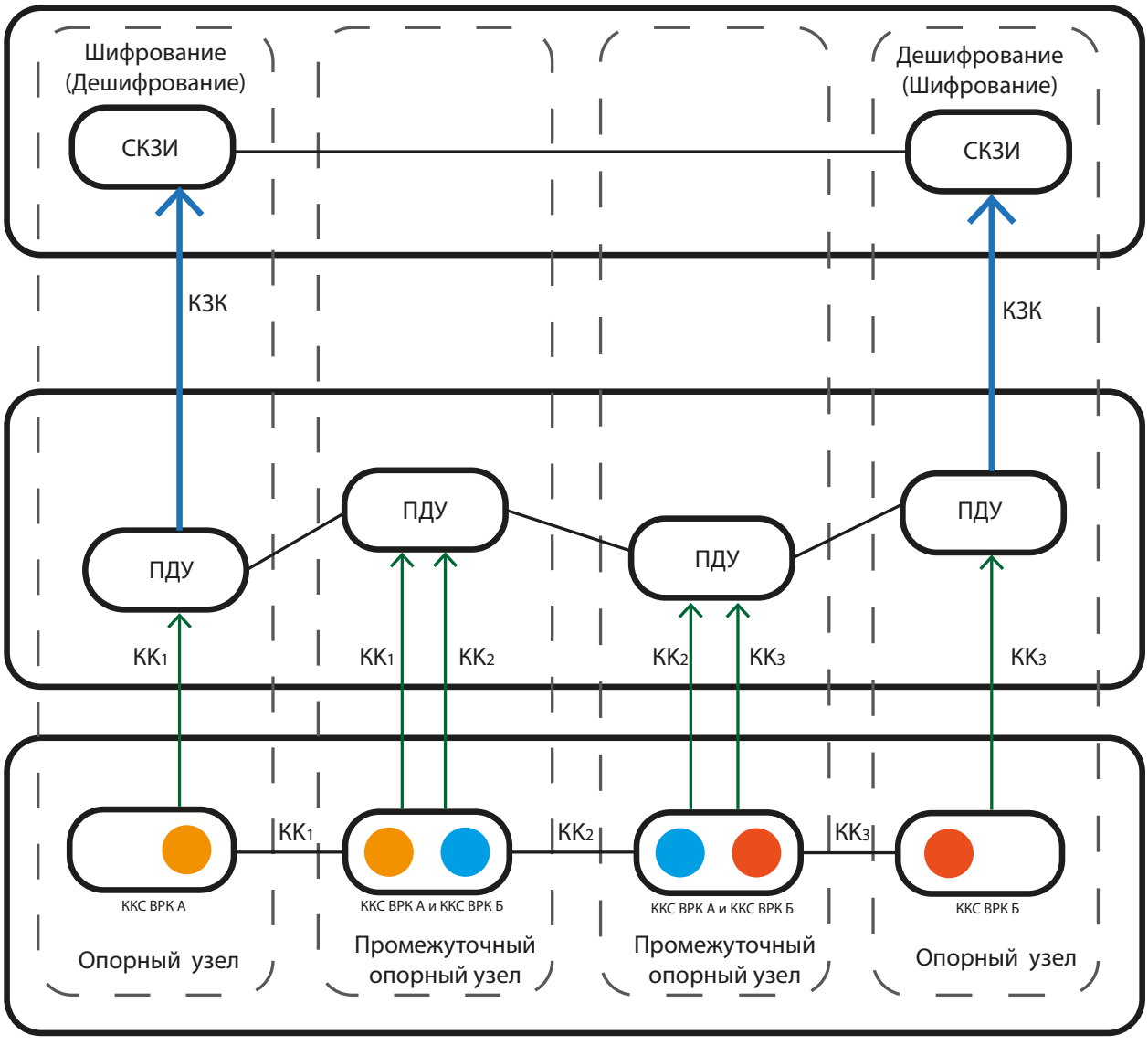

Рис. 4б. Способ организации квантово-защищенной передачи данных, основанный на использовании КЗК для обеспечения шифрования данных, с применением расположенных в опорных узлах СКЗИ

ния данных, с применением расположенных в опорных узлах СКЗИ, КЗК вырабатывается между ОУ методом, включающим ПДУ и рассмотренным в предыдущем разделе. После выработки КЗК осуществляется его доведение до СКЗИ, расположенных в ОУ. Впоследствии данные КЗК используются для шифрования и расшифрования данных, передаваемых между расположенными в ОУ СКЗИ по классическому каналу связи.

Данный метод подразумевает, что КЗК может формироваться и пересылаться между любыми узлами квантовой сети. Также подразумевается, что КЗК в зашифрованном виде может доставляться и до оконечных клиентских узлов (ОКУ), в состав которых не входит один из модулей ККС ВРК и ПДУ. В ОКУ КЗК может доставляться в зашифрованном виде с использованием для шифрования и расшифрования ключей, заранее распределенных между ОКУ и ближайшим к нему узлом квантовой сети, который поддерживает подключение ОКУ (имеет необходимое телекоммуникационное оборудование).

В таком случае КЗК будет доставляться в ОКУ с учетом заранее принятых административных мер, однако это позволит реализовывать защищенное взаимодействие ОКУ со всеми остальными узлами квантовой сети без установки модуля ККС ВРК и ПДУ.

Сравнение двух методов представлено в таблице 2.

Таблица 2

Сравнение методов, основанных на использовании квантовых ключей и квантово-защищенных ключей

Параметр	КК (перешифрование данных)	КЗК (перешифрование ключей)
Защищенность	Высочайшая (только квантовая криптография)	Высокая (за счёт частого обновления ключей – выше, чем сейчас, но не полностью квантовая)
Стоимость	Дороже	Дешевле (экономия на магистральных СКЗИ в узлах)
Наличие модуля КРК у клиента	Обязательно	Необязательно (в простейшем случае только СКЗИ)
Масштабируемость	Сложнее	Проще (КЗК можно доставлять даже в узлы без КРК и ПДУ)
Задержки на перешифрование	Есть (накапливается)	Нет
Маршрут передачи данных	Совпадает с маршрутом выработки ключей	Произвольный
Среда передачи ключей	Только оптика (для КК)	Любая цифровая (для КЗК) и оптика (для КК)

ВЫВОДЫ

В статье рассмотрена методологически важная проблема организации квантово-защищенных сетей для обеспечения безопасного распределения ключей между удаленными абонентами и СКЗИ. Рассмотрен и обоснован конструктивный практический подход к организации квантовых сетей на основе доверенных промежуточных опорных узлов, позволяющий формировать квантово-защищенный ключ между опорными узлами сети на основе квантовых ключей. Показано, что способ организации квантовых сетей, основанный на использовании доверенных ПОУ и квантово-защищенных ключей для обеспечения шифрования данных посредством расположенных в опорных узлах СКЗИ, обладает большим числом преимуществ по сравнению с методом, основанным на применении квантовых ключей для шифрования данных посредством расположенных в каждом узле СКЗИ.

Предлагаемые подходы могут быть использованы для широкого круга квантовых сетей, входящих в состав технологических и финансовых платформ, в том числе предназначенных для хранения и движения цифровых финансовых активов, обслуживания корпоративных систем связи и передачи данных, а также систем распределения и биллинга ключей, корпоративных распределенных реестров.

СПИСОК ЛИТЕРАТУРЫ

1. Козубов А.В., Гайдаш А.А., Кынев С.М., Егоров В.И., Иванова А.Е., Глеим А.В., Мирошниченко Г.П. Основы квантовой коммуникации: часть 1. СПб: Университет ИТМО, 2019. 85 с.
2. Корольков А.В. О некоторых прикладных аспектах квантовой криптографии в контексте развития

квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. 2015. №1 (9). С. 6-13.

3. Егоров В.И., Глейм А.В., Рупасов А.В. Система квантового распределения ключа на поднесущих частотах модулированного излучения с компенсацией искажений сигнала // Ученые записки казанского университета. Серия: физико-математические науки. 2013. №1. С. 59-65.
4. Кузьменко В.В., Макаров В.Л., Разгуляев К.А., Хан Д.В., Черкашин П.А., Щербаков А.Ю. Тенденции развития и практические реализации решений по обеспечению безопасности криптографических сетей // Вестник современных цифровых технологий. 2021. № 6. С. 23-28.
5. Арсланов Н.М., Моисеев С.А. Оптимальные периодические частотные гребенки высокоэффективной оптической квантовой памяти на кристаллах с редкоземельными ионами // Квантовая электроника. 2017. Т. 47, №9. С. 783–789.
6. Разгуляев К.А., Рязанова А.А., Хан Д. В., Щербаков А. Ю. Об одном способе хранения и управления ключами в системах квантовых коммуникаций // Вестник современных цифровых технологий. 2020. № 2. С. 14-20.

УДК: 004.75, 004.41

Конфиденциальное машинное обучение с нулевым разглашением

S.V. Zapechnikov, A.Yu. Shcherbakov

Zero-Knowledge Proofs Privacy-Preserving Machine Learning

Abstract. *The article is devoted to the analysis of a new scientific field – privacy-preserving and verifiable machine learning systems. Such systems allow to generate proof of the correctness for model learning and inference and to verify the proof by the customer of inference task and third parties, which guarantees the integrity of the evaluation process. The main tool for privacy-preserving and verifiable machine computing is zero-knowledge proofs. The article provides an example of a universal purpose zero-knowledge proof system and discusses the main ideas underlying the existing implementations of privacy-preserving and verifiable machine learning systems.*

Keywords: *data mining, machine learning, deep learning, federated learning, confidentiality, secure multi-party computations, secret sharing schemes, homomorphic encryption.*

С.В. Запечников[1]
А.Ю. Щербаков[2]
[1]Доктор технических наук, профессор Института интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ», Вице-президент по научной работе Ассоциации специалистов в области криптовалют и цифровых финансовых активов.
E-mail: SVZapechnikov@mephi.ru
[2]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена анализу положения дел в новой научной области – системах конфиденциального и проверяемого машинного обучения. Такие системы позволяют генерировать доказательства корректности вычислений и обеспечивают возможность проверки доказательства заказчиком вычислений и третьими лицами, что даёт гарантии целостности процесса вычислений. Основным инструментом конфиденциального и проверяемого машинного вычисления являются криптографические доказательства с нулевым разглашением. В статье приводится пример системы доказательства с нулевым разглашением универсального назначения, рассматриваются основные идеи, заложенные в основу существующих реализаций систем конфиденциального и проверяемого машинного обучения.*

Ключевые слова: *интеллектуальный анализ данных, машинное обучение, глубокое обучение, федеративное обучение, конфиденциальность, безопасные многосторонние вычисления, схемы разделения секрета, гомоморфное шифрование.*

ВВЕДЕНИЕ

Конфиденциальное машинное обучение (КМО) – одна из наиболее плодотворных идей в сфере компьютерных наук, появившихся за последние годы. На её реализации в настоящее время сосредоточены усилия множества исследовательских групп в ведущих университетах и IT-корпорациях по всему миру. Это научно-техническое направление возникло на стыке классического машинного обучения и криптографии [1 – 3]. Целью создания систем КМО является реализация новой функциональности – обеспечение возможности решать задачи машинного обучения при условии одновременного обеспечения конфиденциальности данных, предоставляемых для обучения модели, самих обученных моделей, а также данных, передаваемых владельцу обученной модели на этапе её применения для получения решений задач анализа данных. Среди уже имеющихся систем КМО есть конфиденциальные аналоги многих классических методов машинного обучения: метода k средних, решающих деревьев, линейной и логистической регрессий, метода опорных векторов и, конечно, многочисленных вариантов искусственных нейронных сетей (ИНС).

Решение различных задач КМО и развитие технологий в этой области весьма важно для множества областей знания, в первую очередь для аналитических исследований в области конфиденциальных финансовых технологий, когда данные для анализа являются персональными данными, конфиденциальной информацией, либо составляют банковскую тайну. Задачи КМО также необходимо решать

в области цифровых финансовых активов для анализа данных криптобирж и прогнозирования волатильности или трендов развития цифровых активов (криптовалют). Работы в области КМО составляют одну из фундаментальных основ исследований в рамках государственного задания «Исследования в области перспектив развития технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации».

Однако с развитием систем КМО вскоре стало очевидно, что только функции обеспечения конфиденциальности данных для многих практических применений недостаточно. Важна функция обеспечения целостности, в особенности на этапе применения модели, позволяющая заказчику вычислений убедиться в том, что обладатель модели сообщил ему корректный результат решения задачи с использованием как сообщённого заказчиком запроса, так и обученной модели. Обладатель модели также в большинстве случаев заинтересован в том, чтобы обезопасить себя от возможных претензий заказчика, связанных с качеством решения задачи. Таким образом, взаимовыгодным для заказчика вычислений и провайдера модели становится такое свойство систем КМО как проверяемость (верифицируемость) вычислений, позволяющая убедиться в целостности информации, которая служит входом и выходом решения задачи. В ряде систем обеспечивается возможность проверки вычислений не только для заказчика, но и для третьих лиц. Обобщая все аспекты описанного свойства вычислений с моделями КМО, мы предлагаем использовать для него термин «проверяемая целостность», а для систем КМО, обладающих свойствами конфиденциальности и проверяемой целостности, – термин «конфиденциальное и проверяемое машинное обучение» (КПМО).

ПОСТАНОВКА ЗАДАЧИ

Напомним общую идею КМО [3]. Предполагается, что для решения задач пользователя, связанных с анализом данных и обнаружением в них закономерностей, используется некоторая модель машинного обучения. При этом процессы обучения и применения модели происходят дистанционно, т.е. владелец данных и получатель результата с одной стороны, а также обладатель модели с другой стороны – разные лица, взаимодействующие по дистанционным каналам. Обе взаимодействующие стороны заинтересованы в сохранении конфиденциальности своей информации: первый из них желает сохранить в секрете данные, передаваемые для обучения модели, либо запросы, подаваемые к уже обученной модели, второй – параметры обученной модели. Схемы взаимодействия участников показаны на рис. 1 и 2.

В случае, если участники взаимодействия ожидают от системы КМО не только конфиденциальности данных, но и обеспечения свойства проверяемой целостности, им

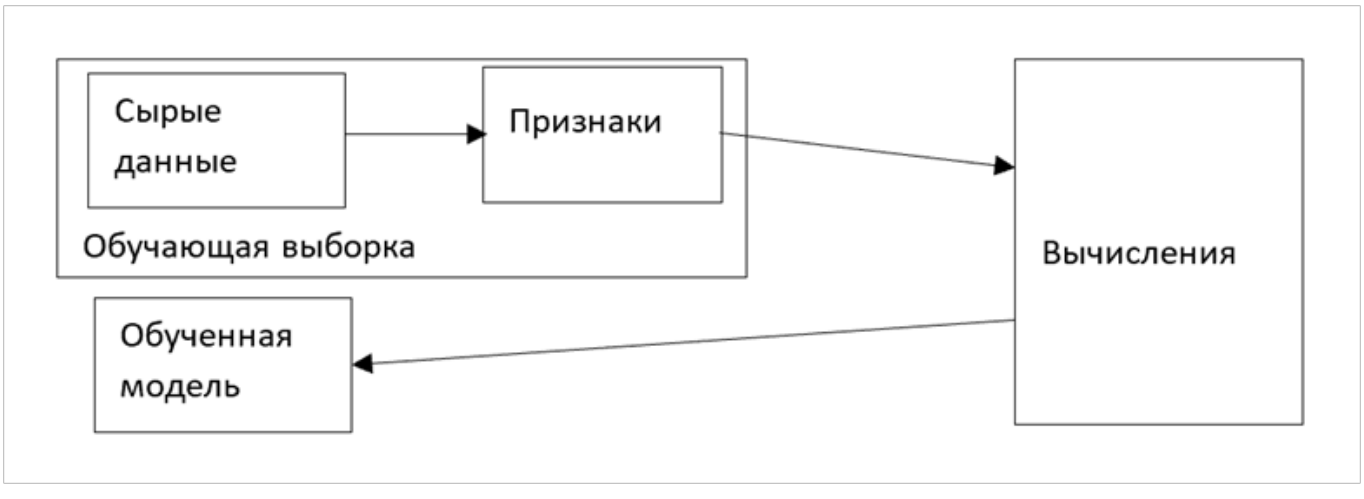

Рис. 1. Взаимодействие участников КМО на этапе обучения

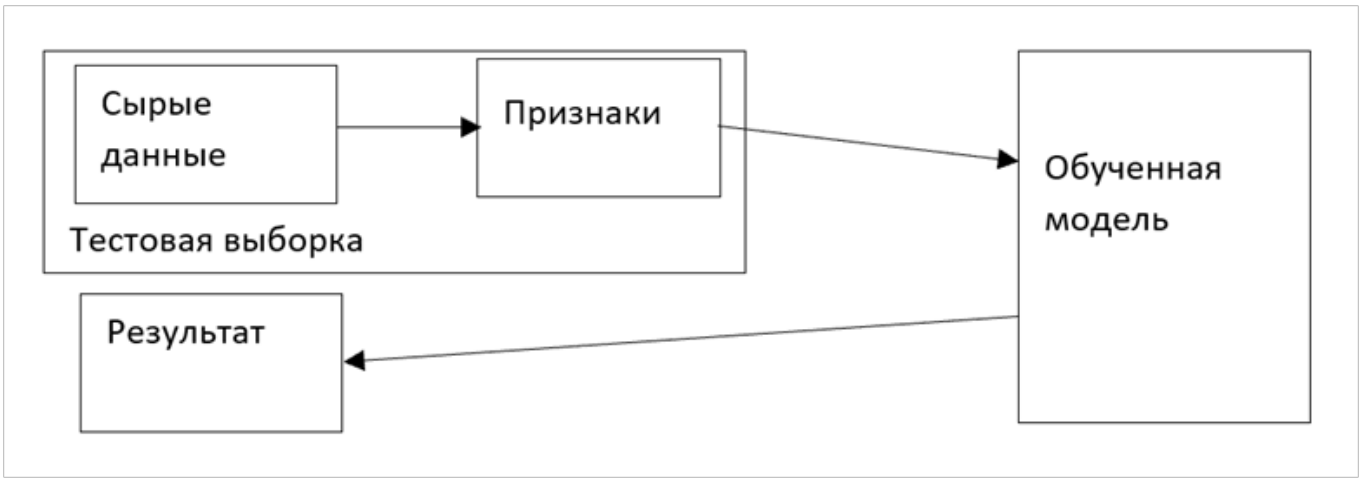

Рис. 2. Взаимодействие участников КМО на этапе применения обученной модели

необходимо дооснастить её дополнительными криптографическими механизмами, чтобы получить систему КПМО. От участников такой системы ожидается следующая функциональность:

- генерация доказательств корректного выполнения алгоритмов обладателем модели.
- прием результатов решения задачи и проверка корректности её решения заказчиком (а если необходимо, то и третьими лицами).

Однако для этого предварительно нужно создать специальный образ модели машинного обучения, называемый коммитментом (commitment). Это специальная структура данных, построенная с использованием криптографических средств, в частности, криптографических функций хэширования или иных однонаправленных функций, которая однозначно связана с исходной конструкцией (например, с ИНС или с решающим деревом), но из которой невозможно восстановить параметры исходной структуры (синаптические веса ИНС или предикаты, ассоциированные с вершинами решающего дерева, соответственно). Коммитменты в большинстве случаев обладают свойствами полноты (completeness), состоятельности (soundness) и статистического сокрытия (hiding) исходных данных.

Обобщая всё сказанное, приведём формальное определение системы КПМО на примере свёрточной ИНС (определение приводится по работе [4].

Пусть W – множество параметров ИНС, $X \in F^{n \times n \times ch}$ – тензор входных данных, где n – размер изображения в пикселях, ch – количество входных каналов, $y = pred(W, X)$ – ответ ИНС на входных данных **X**. Система КПМО для ИНС – это совокупность четырёх алгоритмов:

- алгоритма генерации ключей $KeyGen(1^{\lambda}) \rightarrow pp$, который по заданному параметру безопасности λ генерирует набор общедоступных параметров pp;
- алгоритма генерации коммитмента $Commit(W, pp, r) \rightarrow com_W$, который создаёт коммитмент ИНС с множеством параметров **W**, используя случайность r;
- алгоритма генерации доказательства $Prove(W, X, pp, r) \rightarrow (y, \pi)$, который для заданного тензора **X** вырабатывает при помощи ИНС ответ y и генерирует доказательство целостности π;
- алгоритма проверки доказательства $Verify(com_W, X, y, \pi, pp) \rightarrow \{0,1\}$, который проверяет ответ y, используя коммитмент com_W, доказательство π и входные данные **X**.

Приведенное здесь определение достаточно легко может быть обобщено на КПМО с другими моделями машинного обучения. Дальнейшая задача состоит в конструировании криптосхем, реализующих КПМО. Центральным компонентом таких криптосхем, как следует из определения, являются криптографические системы доказательства с нулевым разглашением (ДНР)

[1] – только они позволяют одновременно обеспечить свойства конфиденциальности и проверяемости вычислений, в связи с чем рассмотрим их подробнее.

СИСТЕМЫ НЕИНТЕРАКТИВНОГО ДОКАЗАТЕЛЬСТВА, ИСПОЛЬЗУЕМЫЕ В КОНФИДЕНЦИАЛЬНОМ МАШИННОМ ОБУЧЕНИИ

Среди всего многообразия ДНР для решения задач КПМО в первую очередь представляют интерес неинтерактивные доказательства, позволяющие доказывать утверждения произвольного вида. Неинтерактивный характер доказательства подразумевает, что они функционируют по аналогии с привычной всем цифровой подписью, т.е. один из участников информационного обмена может сгенерировать доказательство, не привлекая для выполнения этой процедуры никого из других участников, а любое другое заинтересованное лицо, получив такое доказательство, может самостоятельно его проверить и получить однозначное заключение об истинности (или ложности) доказываемого утверждения. Доказательства универсального типа позволяют доказывать утверждения, в которых входные и выходные данные связаны функциями произвольного вида, которые в самом общем случае могут быть выражены арифметическими или, в частном случае, булевыми схемами.

Пусть имеется функция C над некоторым конечным полем F, причем область определения функции C содержит $n+h$ входных переменных из поля F, а область значений функции C содержит l выходных переменных в поле F: $C: F^n \times F^h \to F^l$. Функция C является *арифметической схемой* тогда и только тогда, когда все выходные переменные функции C могут быть определены через входные переменные путем переходов по направленному ациклическому графу, узлы которого ассоциированы с арифметическими операциями сложения и умножения. *Корректным назначением* (valid assignment) для арифметической схемы C будем называть некоторый кортеж $(a_1, \dots, a_N) \in F^N$, где $N = (n+h)+l$ такой, что $C(a_1, \dots, a_{n+h}) = (a_{n+h+1}, \dots, a_N)$.

В наибольшей степени перечисленным условиям соответствует класс криптографических систем доказательства, называемых компактными неинтерактивными доказательствами знания с нулевым разглашением (zk-SNARK – zero-knowledge succinct non-interactive arguments of knowledge). В настоящее время при проектировании систем безопасных многосторонних вычислений, в частности, систем КПМО, используется несколько систем zk-SNARK. Рассмотрим в качестве примера систему, описанную в работе [5].

Для этого рассмотрим центральное этой системы доказательства понятие *квадратичной арифметической программы* (QAP – quadratic arithmetic program). Пусть имеется функция $Q(C) := (\vec{A}, \vec{B}, \vec{C}, Z)$, где $Z(z) \in F[z]$ будем называть целевым полиномом, а тройка векторов $\vec{A}, \vec{B}, \vec{C}$ определяется следующим образом:

$$\vec{A} = (A_i(z))_{i=0}^{m}, \vec{B} = (B_i(z))_{i=0}^{m}, \vec{C} = (C_i(z))_{i=0}^{m}, где z \in Fum \geq N.$$

Далее определяется полином $P(z) = \left(A_0(z) + \sum_{i=1}^{m} a_i A_i(z)\right)\left(B_0(z) + \sum_{i=1}^{m} a_i B(z)\right) - \left(C_0(z) + \sum_{i=1}^{m} a_i C(z)\right)$ такой, что $Z(z)$ делит полином $P(z)$ тогда и только тогда, когда кортеж $(a_1, \dots, a_N)$ является корректным назначением для C.

Квадратичная арифметическая программа в zk-SNARK используется для того, чтобы доказывающий **P** сконструировал доказательство π, подтверждающее знание $(a_1, \dots, a_N) \in F^N$ для арифметической схемы C. Имея доказательство π, проверяющий **V** достаточно легко может проверить делимость $P(z)$ на $Z(z)$.

Рассмотрим теперь метод построения QAP для арифметической схемы **C**. Пусть арифметической схеме **C** соответствует такой направленный ациклический граф, концевые вершины которого определены только через операции умножения. Определим **m** как суммарное количество рёбер, входящих в некоторую вершину графа и исходящих из него.

Пусть **M** – подмножество вершин графа, **W** – множество входящих ребер для подмножества вершин **M**. Для узла $g \in M$ введем обозначение

$I_{g,L} \subset W$ для подмножества ребер, входящих слева для узла **g**. Соответственно, $I_{g,R} \subset W$ – подмножество ребер, входящих справа для узла **g**. Далее определим целевой полином $Z(z)$ для вершин схемы **C**: $Z(z) = \prod_{g \subset M}(z - r_g)$.

Наконец, определим полиномы для векторов $\vec{A} u \vec{B}$ следующим образом:

$$A_i(r_g) = c_{g,L,i}, если i \in I_{g,L}, иначе A_i(r_g) = 0,$$

$$B_i(r_g) = c_{g,R,i}, если i \in I_{g,R}, иначе B_i(r_g) = 0.$$

где $c_{g,L,i}$ – скалярный множитель, с которым ребро i входит в узел **g** слева. Также введем обозначения $A_0(r_g)$ и $B_0(r_g)$ для констант, входящих в узел g слева и справа соответственно.

Определим полином для вектора $\vec{C}$ следующим образом:

$$C_i(r_g) = 1, если i = g, иначе C_i(r_g) = 0.$$

Таким образом, получаем следующие правила полиномиального представления арифметической схемы:

1) входящее значение для узла g слева:

$$A(r_g) = A_0(r_g) + \sum_{i=1}^{m} a_i A_i(r_g) =$$

$$A_0(r_g) + \sum_{i \in I_{g,L}} a_i c_{g,L,i};$$

2) входящее значение для узла **g** справа:

$$B(r_g) = B_0(r_g) + \sum_{i=1}^{m} a_i B_i(r_g) =$$

$$B_0(r_g) + \sum_{i \in I_{g,R}} a_i c_{g,R,i};$$

3) исходящее значение для узла **g**:

$C(r_g) = C_0(r_g) + \sum_{i=1}^{m} a_i C_i(r_g) = a_g$.

Для всех $g \in M$ это означает, что полином

$P(r_g) = A(r_g) \cdot B(r_g) - C(r_g) = 0$.

Таким образом, кортеж $(a_1, \dots, a_N)$ является корректным назначением для арифметической схемы C, тогда и только тогда, когда $P(z)$ имеет нули для всех r_g что эквивалентно делимости $P(z)$ на $Z(z)$.

Введем дополнительные обозначения. Пусть R_c – пара векторов $(\vec{x}, \vec{w})$ с нулевым выходом, которая образует корректное назначение для арифметической схемы C:

$$R_c = \{(\vec{x}, \vec{w}) | \in F^n \times F^h | C(\vec{x}, \vec{w}) = 0\}$$

Пусть L_C – NP-полный язык для векторов $\vec{x}$, которые могут образовать корректные назначения с нулевым выходом с некоторыми векторами $\vec{w}$:

$$L_c = \{\vec{x} \in F^n \vee \exists \vec{w} \in F^h : C(\vec{x}, \vec{w}) = 0\}$$

В этом случае будем называть $\vec{w}$ свидетельством (witness), которое будет являться секретом доказывающего P.

Практическая реализация такой системы доказательства zk-SNARK основывается на использовании билинейных отображений вида $e: G_1 \times G_2 \to G_T$, где G_1 и G_2 – циклические группы с образующими элементами $P_1 \in G_1$ и $P_2 \in G_2$ соответственно, G_T – группа порядка r.. Отображение e – невырожденное несимметричное (т.е. $G_1 \neq G_2$ билинейное отображение, удовлетворяющее условиям:

$e(n_1 P_1, n_2 P_2) = e(P_1, P_2)^{n_1 n_2}$ и $e(P_1, P_2) \neq 1$.

Рассмотрим свойства zk-SNARK: полноту (completeness), состоятельность (soundness) и нулевое разглашение (zero-knowledge).

Полнота означает, что проверяющий V всегда примет доказательство корректного утверждения. Пусть полиномы QAP были сгенерированы на предыдущем этапе. Для обеспечения полноты доказательства при его генерции выполняются следующие шаги.

Шаг 1. Генерация ключей.

1. Определить арифметическую схему $C: F^n \times F^h \to F^l$.
2. Определить QAP: $Q(C) = (\vec{A}, \vec{B}, \vec{C}, Z)$.
3. Сгенерировать ключи доказательства. Для этого выбрать случайные $\tau, \rho_A, \rho_B \in F$. Пусть $\rho_c := \rho_A \rho_B$, где $pk_A := (A_i(\tau)\rho_A P_1)_{i=1}^m, pk_B := (B_i(\tau)\rho_B P_2)_{i=1}^m, pk_C := (C_i(\tau)\rho_C P_1)_{i=1}^m$, $pk_H := (\tau P_1)_{i=1}^d$.
4. Сгенерировать ключ проверки $vk_{IC} := (A_i(\tau)\rho_A P_1)_{i=1}^n vk_Z := (Z(\tau)\rho_C P_2)$.

В результате выполнения шага 1 создаются ключи доказательства и ключи проверки.

Шаг 2. Создание доказательства.

1. Определить QAP: $Q(C) = (\vec{A}, \vec{B}, \vec{C}, Z)$.
2. Вычислить валидное распределение $(a_1, \dots, a_m = QAPwit(C, \vec{x}, \vec{w})$.
3. Определить коэффициенты $h_{i\,i=0}^{d}$ многочлена $H(z) = \frac{A(z)B(z)-C(z)}{Z(z)}$.
4. Вычислить доказательство $\pi := (\pi_A, \pi_B, \pi_C, \pi_H)$, где

$\pi_A := \sum_{i=1}^m a_i pk_{A,i}, \pi_B := pk_{B,0} + \sum_{i=1}^m a_i pk_{B,i}, \pi_C := pk_{C,0} + \sum_{i=1}^m a_i pk_{C,i}$, $\pi_H := pk_{H,0} + \sum_{i=1}^d h_i pk_{H,i}$.

Доказательство π_H кодирует полином

$H(z)$ элементами группы G, т.е. $\pi_H = H(\tau) \cdot \rho_B P_1$. Соответственно, π_B кодирует полином $B(z)$, т.е. $\pi_B = (B_0(\tau) + \sum_{i=1}^{m} a_i B_i(\tau))H(\tau) \cdot \rho_B P_2$.

5. На следующем шаге проверяющий V выполняет деление $P(z)$ на $Z(z)$. Для этого вычислять $vk_{\vec{x}} = vk_{IC,0} + \sum_{i=1}^{n} x_i vk_{IC,i}$.

6. Далее проверить делимость $P(z)$ на $Z(z)$, т.е. тот факт, что $e(vk_{\vec{x}} + \pi_A, \pi_B) = e(\pi_H, vk_z) \cdot e(\pi_C, P_2)$.

Состоятельность означает, что доказывающий сможет убедить проверяющего принять доказательство ложного утверждения лишь с пренебрежимо малой вероятностью.

Нарушитель может использовать $P(z) = Z(z)$ в качестве своего доказательства с $A(z) = 1, B(z) = Z(z) u C(z) = 0$. Такие значения могут быть приняты проверяющим V даже в случае, если доказывающий P не знает корректное назначение $(\vec{x}, \vec{w}) \in R_C$. Таким образом, проверяющий V также должен выполнить две проверки:

- проверку того, что полиномы $A(z), B(z) u C(z)$ являются линейными комбинациями $\vec{A}$, $\vec{B} u \vec{C}$ соответственно;
- проверку того, что линейная комбинация $\vec{A}$, $\vec{B} u \vec{C}$ использует одинаковые коэффициенты a_i.

Такая проверка достигается посредством построения доказывающим второго аналогичного доказательства с использованием отличающихся ключей путем перемножения на некоторый случайный коэффициент α_A: $pk'_{A,i} = \alpha_A pk_{A,i}$. Доказывающий не знает α_A, однако может вычислить $\pi'_A = \alpha_A \pi_A$, для чего должны быть использованы $pk'_{A,i}$ и $pk_{A,i}$.

Таким образом, необходимо выполнить следующие шаги:

Шаг 1. Генерация ключей.

1.1. Генерация ключей для проверки наличия линейных комбинаций:

1) выбрать случайные элементы поля $\alpha_A, \alpha_B, \alpha_C \in F$;

2) вычислить ключи доказывающего P:
$pk'_{A,i} := (\alpha_A A_i(\tau) \rho_A P_1)_{i=1}^{m}$,
$pk'_{B,i} := (\alpha_B B_i(\tau) \rho_B P_1)_{i=1}^{m}$,
$pk'_{C,i} := (\alpha_A C_i(\tau) \rho_C P_1)_{i=1}^{m}$;

3) вычислить ключи проверяющего V:
$vk_A := \alpha_A P_2, vk_B := \alpha_B P_2, vk_C := \alpha_C P_2$.

1.2. Генерация ключей для проверки использования одинаковых коэффициентов:

1) выбрать случайные элементы поля $\beta, \gamma \in F$;

2) вычислить ключи доказывающего P: $pk_K =$;

3) вычислить ключи проверяющего V: $vk_\gamma := \gamma P_2, vk^1_{\beta\gamma} := \gamma\beta P_1, vk^2_{\beta\gamma} := \gamma\beta P_2$.

Шаг 2. Проверка наличия линейных комбинаций.

Доказывающий P добавляет к доказательству π: $\pi'_A := \sum_{i=n+1}^{m} a_i pk'_{A,i}$, $\pi'_B := pk'_{B,0} + \sum_{i=n+1}^{m} a_i pk'_{B,i}$, $\pi'_C := pk'_{C,0} + \sum_{i=n+1}^{m} a_i pk'_{C,i}$.

Проверяющий может использовать это доказательство для того, чтобы проверить равенства:

$e(\pi_A, vk_A) = e(\pi'_A, P_2)$, $e(\pi_B, vk_B) = e(\pi'_B, P_2)$, $e(\pi_C, vk_C) = e(\pi'_C, P_2)$.

Учитывая, что равенства выполняются если и только если $\pi'_A = \alpha_A \pi_A$, можно утверждать, что доказывающий P использовал для вычислений ключи $pk_{A,i}$ и $pk'_{A,i}$, принадлежащие A.

Шаг 3. Проверка наличия коэффициентов.

Доказывающий добавляет к доказательству π выражение $\pi_K := pk_{K,0} + \sum_{i=1}^{m} a_i pk_{K,i}$. Далее проверяющий V выполняет проверку равенства: $e(\pi_K, vk_\gamma) = e(vk_{\vec{x}} + \pi_A + \pi_C, vk^2_{\beta\gamma}) \cdot e(vk^1_{\beta\gamma}, \pi_B)$. Следовательно, при положительном результате проверки доказывающий P должен был использовать одинаковые коэффициенты a_i для вычисления $\pi_A, \pi_B u \pi_C$, чтобы эти равенства выполнялись.

Нулевое разглашение означает, что доказывающий может использовать $\sigma_1, \sigma_2 u \sigma_3 \in F$ и изменить полиномы в QAP на следующие:
$A(z) = A_0(z) + \sum_{i=1}^{m} a_i A_i(z) + \sigma_1 Z(z)$,
$B(z) = B_0(z) + \sum_{i=1}^{m} a_i B(z) + \sigma_2 Z(z)$,
$C(z) = C_0(z) + \sum_{i=1}^{m} a_i C(z) + \sigma_3 Z(z)$.

В этом случае информация о корректном назначении $(a_1, \dots, a_m)$ остается скрытой, при этом сохраняется свойство делимости полинома $P(z)$ на $Z(z)$.

Имеется целый ряд эффективных реализаций систем zk-SNARK, которые отличаются между собой главным образом методикой использования билинейных отображений при генерации доказательства и, соответственно, алгоритмами проверки таких доказательств. Самыми

известными и эффективными из них являются системы Грота [6] и Грота – Маллер [7], которые выбираются в большинстве случаев создателями систем КПМО.

РЕАЛИЗАЦИЯ СИСТЕМ КОНФИДЕНЦИАЛЬНОГО И ПРОВЕРЯЕМОГО МАШИННОГО ОБУЧЕНИЯ

Будем рассматривать реализации систем КПМО согласно хронологии их появления. Все решения относятся к периоду 2019 – 2021 гг. Большинство известных реализаций систем КПМО направлено на обеспечение свойств конфиденциальности и проверяемой целостности для ИНС. Это легко объяснимо, поскольку ИНС – самый популярный и распространенный инструмент машинного обучения. Однако будут встречаться и исключения из этого правила.

Система VeriML [8] является, пожалуй, самой ранней попыткой обеспечить одновременно конфиденциальность и проверяемость ИНС при помощи SNARK (но без свойства нулевого разглашения). Идея схемы состоит в том, что доказывающий создает коммитменты всех слоёв ИНС, а проверяющий случайным образом выбирает какой-то один слой для проверки и проверяет корректность его вычисления при помощи криптографического доказательства. Очевидно, что такая схема не способна обеспечивать свойство состоятельности доказательства. Она слишком сложна и малопроизводительна для того, чтобы с её помощью можно было проверять вычисления ответа на запрос к ИНС целиком. В связи с этим мы оставим эту систему за рамками дальнейшего рассмотрения.

Система vCNN [9] явилась одной из первых попыток создать систему КПМО. Ключевая идея авторов системы состоит в построении оптимизированных арифметических схем для выполнения операций свёртки, которые занимают до 90% времени выполнения операций при применении обученной свёрточной ИНС. Предложенный способ пригоден для свёрточных ИНС с нелинейными функциями активации ReLU и слоями пулинга. В качестве системы ДНР в ней используется конструкция Грота [6]. Авторы протестировали свою разработку на ИНС VGG16 и получили условно приемлемое время генерации доказательства – 8 часов при объёме общей ссылочной строки доказывающего и проверяющего (CRS – common reference string) около 80 ГБ. Главное значение этой работы состоит в том, что она была первой, в которой был указан путь снижения сложности процедур генерации и проверки ДНР для таких сложных схем как ИНС с «астрономической», находящейся далеко за гранью возможностей современной вычислительной техники, до условно практически приемлемой. На текущий момент система vCNN уступает более новым решениям по производительности и стойкости. Вслед за ней довольно быстро появились другие системы, которые превосходят её по скорости генерации доказательств и их объёму на несколько порядков величины. Далее рассмотрим эти решения более подробно.

Единственной в своём роде системой КПМО для важнейшего из неградиентных методов машинного обучения – метода решающих деревьев является система, описанная в работе [10]. Она предназначена для использования на этапе применения обученного решающего дерева, обеспечивая конфиденциальность как данных, подаваемых на вход модели, так и предикатов, ассоциированных с узлами дерева. Идея построенная конфиденциальной и проверяемой модели на основе решающего дерева заключается в следующем.

На фазе инициализации системы создается коммитмент решающего дерева. Эта процедура выполняется за время, линейно зависящее от размера решающего дерева. Для этого используется специальная структура данных – аутентифицированное решающее дерево, которое однозначно связано с исходным решающим деревом, но из которого невозможно восстановить его параметры за счёт хэширования данных, ассоциированных с листьями, промежуточными вершинами и «подмешивания» случайной величины к хэш-коду корня.

На этапе применения решающего дерева для получения ответа на запрос процедура будет иной: обладатель модели выступает в роли доказывающего, инициатор запроса (он же заказчик ответа) – в роли проверяющего. Доказательство, прилагаемое вычислителем к ответу, является неинтерактивным. Для его построения

используются как те данные, которые доступны обеим сторонам, так и те данные, которые известны только доказывающему и которые он не намерен раскрывать проверяющему. К первым относятся запрос, ответ и коммитмент дерева. Ко вторым – путь, пройденный по дереву от корня к одному из листьев при вычислении ответа, а также случайность, подмешанная к корню дерева при создании коммитмента. Для повышения производительности схемы при генерации доказательства может также добавляться вектор-перестановка вектора входных признаков и вектор хэш-кодов вершин дерева, соседних с вершинами, составляющими путь, пройденный при получении ответа (siblings). Окончательно доказательство получается как совокупность выражений, подтверждающих, что при получении ответа был полностью использован вектор входных признаков (точнее, некоторая перестановка компонентов этого вектора), путь по дереву пройден полностью от корня до одного из листьев и при вычислении ответа использовано в точности то же самое дерево, для которого на фазе инициализации был получен коммитмент.

Авторы работы также предлагают специальную схему доказательства, при помощи которой заказчик может убедиться, что предлагаемая ему для предсказания ответа модель соответствует заявленной (или ожидаемой) точности (accuracy) на тестовой выборке.

В качестве неинтерактивной системы ДНР для описанной конструкции выбрана система Aurora [11]. Обладающая постквантовой стойкостью. Схема может быть распространена на часто используемые разновидности моделей машинного обучения, производные от решающих деревьев: дерево для решения задачи регрессии и случайный лес.

В работе [12] предложена и реализована система КПМО для свёрточных ИНС. Основная идея системы ZEN заключается в построении цепочки алгоритмов (toolchain), которая позволяет построить верифицируемую ИНС, обрабатывающую числа с плавающей запятой за практически приемлемое время. Основные звенья этой цепочки – это:

- способ квантования чисел с плавающей запятой – превращения их в целые числа без знака, удобный для обработки их в ИНС с функциями конфиденциальности и проверяемости вычислений;
- способ кодирования векторов целых чисел без знака, обеспечивающий удобство их параллельной обработки при вычислении скалярных произведений и матричном умножении;

При этом авторами одновременно преодолён целый ряд препятствий, ранее не позволявших получить практически приемлемые показатели функционирования таких систем.

Первая из решённых в этой работе проблем заключается в том, что существующие ИНС обрабатывают числа с плавающей запятой, в то время как все существующие системы ДНР предполагают арифметические вычисления над конечными полями. Таким образом, ИНС оказываются несовместимы с ДНР. Существующие алгоритмы квантования чисел с плавающей запятой не подходят, так как требуют операций деления и оставляют часть данных числами с плавающей запятой. В связи с этим авторы предложили новый способ квантования, который позволяет построить ИНС, обрабатывающую только целые числа без знака, которые уже можно интерпретировать как элементы конечного поля. Предложенный способ квантования позволяет вычислять нелинейные функции активации слоёв ИНС типа ReLU и “average pool” (пулинг по среднему значению).

Вторая проблема состоит в том, что большинство известных квантованных ИНС способны обрабатывать лишь 8-битные целые числа, но большинство ДНР используют эллиптические кривые над полем порядка $\approx 2^{254}$, что приводит к неэффективной реализации. В связи с этим авторы предложили новый метод кодирования данных для обработки в ИНС – так называемое скрученное кодирование (stranded encoding), которое позволяет упаковывать множество переменных в один вектор и выполнять множество операций умножения элементов конечного поля в одном пакете, тем самым многократно ускоряя матричные операции.

В качестве системы ДНР в ZEN используется широко известная система Грота [6], основанная на билинейных отображениях над группами точек эллиптических кривых.

Авторы реализовали свою разработку в виде пакета программ с открытым исходным кодом. Для тестирования ими были взяты нейронные сети ShallowNet, LeNet-5 и LeNet-Face (последняя оптимизирована для решения задач распознавания лиц). В качестве тестовых массивов данных брались широко известные датасеты MNIST, CIFAR-10 и ORL. Созданные программы позволяют построить системы конфиденциальной и проверяемой классификации и распознавания. Под классификацией здесь понимается классическая задача позиционирования объекта, детектированного на изображении, как относящегося к одному из нескольких предопределённых классов. Под распознаванием – сравнение двух изображений и вынесение решения о том, относятся или нет они к одному и тому же классу (в частности, распознавание двух изображений лица как принадлежащих одному человеку). Система ZEN предназначена для использования только на этапе применения обученной ИНС (inference), но не на этапе обучения.

Обе схемы, как показано авторами, обладают свойствами полноты, состоятельности и нулевого разглашения, хотя определения этих свойств для двух систем несколько различаются. Показано, что предложенные методы не влияют существенным образом на точность (accuracy) решения задач по сравнению с обычными ИНС, не обладающими свойствами конфиденциальности и проверяемой целостности.

В качестве ограничений системы ZEN следует указать, прежде всего, ограниченную масштабируемость (испытания проводились на далеко не самых сложных из современных свёрточных ИНС и не самых обширных массивах данных), отсутствие исследований возможности её применения к иным типам ИНС, помимо свёрточных, отсутствие возможности сокрытия от постороннего наблюдателя архитектуры ИНС.

В работе [4] предложена ещё одна система КПМО для свёрточной ИНС, названная авторами zkCNN. Ключевая особенность этой системы – использование быстрого преобразования Фурье (БПФ) для вычисления свёрток, в связи с чем для эффективного вычисления и проверки криптографических доказательств авторы предлагают новый алгоритм вычисления контрольных сумм (sumcheck) для БПФ. Алгоритм позволяет добиться логарифмического времени генерации и проверки доказательств.

В zkCNN используется обобщение неинтерактивной системы доказательства GKR (Goldwasser – Kalai – Rothblum) [13], оптимизированное для свёрточных ИНС. zkCNN поддерживает вычисление нелинейных функций активации ReLU и пулинг по максимальному значению.

Тестирование системы zkCNN, проведённое на ИНС VGG16 с 15 миллионами параметров на датасете CIFAR-10 показало среднее время генерации доказательств 163 с и среднее время их проверки 172 мс при объёме доказательства 230 КБ, что, по утверждению авторов, на три порядка быстрее лучшей из ранее известных схем.

В работе [14] представлена система Mystique, в которой на единой платформе предложено решение сразу несколько задач, остающихся актуальными для КПМО. Разработка позволяет переключаться между арифметическими и булевыми схемами (что удобно и необходимо при вычислении линейных преобразований ИНС), числами с плавающей и с фиксированной запятой (что актуально при вычислении нелинейных преобразований), коммитментами и конфиденциальными данными (что позволяет настраивать степень конфиденциальности системы под требования заказчика), интегрируя их все в вычислительную схему, для которой генерируется доказательство. Таким образом, эта система позволяет, в том числе, скрывать от посторонних лиц архитектуру модели машинного обучения. Авторами также представлен оптимизированный протокол DHP для матричного умножения, который даёт 7-кратный рост производительности по сравнению с лучшими из известных алгоритмов. Все перечисленные свойства достигаются за счёт несущественного (около 0,2%) снижения точности моделей по сравнению с исходными. Система Mystique интегрирована в фреймворк Rosetta, предназначенный для реализации КМО и основанный на библиотеке TensorFlow.

ЗАКЛЮЧЕНИЕ

В статье проведен обзор всех известных (по состоянию на июнь 2021 г.) систем КПМО. Выявлено, что основным криптографическим инструментом для конструирования таких систем служат компактные неинтерактивные доказательства знания с нулевым разглашением (zk-SNARK).

Нет сомнений в том, что системы КМО и КПМО будут активно востребованы в будущем. Рассмотренные в статье системы, скорее всего, в недалеком будущем станут считаться лишь первыми шагами по пути их практической реализации. Все описанные системы пока являются экспериментальными образцами, для их широкого практического применения необходимо решить целый ряд проблем.

Среди основных нерешённых проблем можно отметить следующие:

- относительно низкая производительность систем КПМО, ограничивающая сферу их применения лишь высокопроизводительными вычислительными устройствами;
- весьма ограниченная применимость всех известных методов на этапе обучения моделей;
- невозможность существующими средствами обеспечить конфиденциальность архитектуры ИНС – все известные системы КПМО скрывают лишь параметры ИНС, считая все элементы её архитектуры (количество слоёв, каналов, нейронов, конфигурацию связей между слоями и пр.) общеизвестными.

Представляется, что дальнейшее развитие КМО будет в значительной мере связано с решением перечисленных научно-практических задач, что позволит широко применить их в области цифровых финансовых активов, когда необходимо анализировать данные криптобирж, прогнозировать волатильность или тренды развития цифровых активов (криптовалют).

СПИСОК ЛИТЕРАТУРЫ

1. Запечников С.В. Криптографическая защита процессов обработки информации в недоверенной среде: достижения, проблемы, перспективы // Вестник современных цифровых технологий. 2019. №1. С. 6 – 18.

2. Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий. 2020. Т. 27, Вып. 1. С. 51–67.

3. Запечников С.В. Доказательства с нулевым разглашением и их применения при обработке информации в недоверенных средах // Вестник современных цифровых технологий. 2021. №6. С. 11 – 22.

4. Liu T., Xie X., Zhang Y. zkCNN Zero knowledge proofs for convolutional neural network predictions and accuracy. URL: https://eprint.iacr.org/2021/673 (дата обращения: 07.06.2021).

5. Parno B., Howell J., Gentry C., Raykova M. Pinocchio: Nearly Practical Verifiable Computation // IEEE Symposium on Security and Privacy. 2013. Pp. 238-252. doi: 10.1109/SP.2013.47.

6. Groth J. On the Size of Pairing-Based Non-interactive Arguments // Advances in Cryptology – EUROCRYPT 2016. Lecture Notes in Computer Science. Vol. 9666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49896-5_11

7. Groth J., Maller M. Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs // Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science. Vol. 10402. Springer, Cham. https://doi.org/10.1007/978-3-319-63715-0_20

8. Zhao L., Wang Q., Wang C., et al. VeriML: Enabling Integrity Assurances and Fair Payments for Machine Learning as a Service. URL: https://arxiv.org/pdf/1909.06961v1.pdf

9. Lee S., Ko H., Kim J., Oh H. vCNN: Verifiable convolutional neural network based on zk-SNARKs. URL: https://eprint.iacr.org/2020/584 (дата обращения: 07.06.2021).

10. Zhang J., Fang Z., Zhang Y., Song D. Zero knowledge proofs for decision tree predictions and accuracy // CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security,

2020. P. 2039–2053. Doi: 10.1145/3372297.3417278.

11. Ben-Sasson E., Chiesa A., Riabzev M. et al. Aurora: Transparent Succinct Arguments for R1CS // Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Springer. Vol. 11476. P. 103-121. Doi: 10.1007/978-3-030-17653-2_4.

12. Feng B., Qin L., Zhang Z. et al. ZEN: An optimizing compiler for verifiable, zero-knowledge neural network inferences. URL: https://eprint.iacr.org/2021/087 (дата обращения: 07.06.2021).

13. Goldwasser S., Kalai Y., Rothblum G. Delegating Computation: Interactive Proofs for Muggles. Journal of ACM. Vol. 62, No. 4. Article 27 (Sept. 2015). Pp. 1-64.

14. Weng C., Yang K., Xie X. et al. Mystique: Efficient conversions for zero-knowledge proofs with applications to machine learning. URL: https://eprint.iacr.org/2021/730 (дата обращения: 07.06.2021).

УДК: 004.03, 004.7

Обоснование свойств цифровых платформ в рамках субъектно-объектной модели компьютерных систем

A.A. Ryazanova

The Substantiation of the Properties of Digital Platforms in the Framework of the Subject-Object Model of Computer Systems

Abstract. *The article discusses the basic concepts and properties of digital platforms from the viewpoint of the theoretical subject-object model of computer systems. The substantiation of the relationship between the properties of flows and processes of generation of subjects of a computer system with the properties of integrability and development of digital platforms is given. The influence of the properties of the digital platforms based on the subject-object model on the integrability of the information processes is described.*

Keywords: *subject-object model, digital platform, integrability of the digital platforms, property of development, flow transitivity, processes integration.*

А.А. Рязанова[1]
[1]Научный сотрудник ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: a.ryazanova@c3da.org

Аннотация. *В статье рассматриваются основные понятия и свойства цифровых платформ с позиций теоретической субъектно-объектной модели компьютерных систем. Приводится обоснование взаимосвязи свойств потоков и процессов порождений субъектов компьютерной системы со свойствами интегрируемости и развития цифровых платформ. Описывается влияние свойств цифровых платформ, основанных на субъектно-объектной модели, на интегрируемость процессов в рамках цифровых платформ.*

Ключевые слова: *субъектно-объектная модель, цифровая платформа, интегрируемость цифровых платформ, свойство развития, транзитивность потоков, интеграция процессов.*

ВВЕДЕНИЕ. СУБЪЕКТНО-ОБЪЕКТНАЯ МОДЕЛЬ КОМПЬЮТЕРНЫХ СИСТЕМ

В современных информационных технологиях модель компьютерной системы (КС) рассматривается исходя из положений системного анализа в виде множества взаимодействующих элементов и компонент, которое включает два подмножества: множество объектов и множество субъектов. Эта модель, дополненная функциями потока и порождения субъектов, на сегодняшний день стала общепринятой и называется субъектно-объектной моделью КС (СО-модель) [1].

Разделение на субъекты и объекты основано на свойстве элемента компьютерной системы «быть активным» или «получать управление», исторически сложившемся на основе модели вычислительной системы фон Неймана [2], согласно которой последовательность исполняемых инструкций для вычисляющего блока (процессора) (программа, рассматриваемая как «субъект» компьютерной системы) и данные, выступающие в качестве «объекта», находятся в одной среде. При этом программа является и системной целостностью, и системообразующим компонентом КС.

Вместе с тем, в современном дискурсе в области информационных технологий наряду с понятием компьютерной системы закрепляется более глубокое и емкое понятие- понятие платформы. Это связано с тем, что компьютерная система имеет достаточно узкое назначение (целевую функцию), в то время как понятие платформы подразумевает наличие двух основных диалектических свойств – развития и интегрируемости [3].

Напомним, что свойство развития обеспечивает переход от количественных показателей к качественным и проявляется, например, при обработке больших данных, а свойство интегрируемости включает возможность интеграции как «сверху» (платформа может быть основой для построения на ней некоторой целевой масштабируемой, тиражируемой и расширяемой архитектуры), так и «снизу» (платформа может технологически «опираться» на другую или другие взаимодействующие с ней платформы).

При этом реализация как свойства развития, так и свойства интегрируемости возможна ис-

ключительно на уровне активной компоненты - субъектов, что позволяет сформировать новый взгляд на СО-модель и является дополнительным подтверждением ее важнейшего фундаментального значения для теоретического осмысления базовых понятий цифровых платформ.

Таким образом, в применении к цифровым платформам (ЦП) элементами системы будут являться субъекты и объекты, однако сама цифровая платформа будет отличаться как составом и структурой, так и количеством взаимосвязей.

Основное свойство субъектов в цифровой платформе заключается в том, что пользователь ЦП воспринимает данные (объекты) и получает информацию, обрабатываемую и хранимую в рамках платформы, только через субъекты, которыми он управляет.

Программа в ЦП предназначена для решения законченной задачи, сформулированной ее разработчиком. Модули же, как подсистемы, решают отдельные подзадачи, имеют минимальный размер и одну точку входа и выхода, а также не зависят от типа реализации других модулей. Например, программа Microsoft Word, предназначенная для полнофункциональной работы с текстами и электронными документами, включает множество программных модулей. В ЦП в обязательном порядке должны быть предусмотрены процессы как формирования документов, так и их отсылки другим участникам цифровой платформы, либо в систему хранения ЦП.

Передача информации от субъектов верхнего уровня (которыми управляют пользователи ЦП) происходит иерархически. Например, по команде участника системы в меню программы текстового редактора «Сохранить файл» набранный в редакторе текст передается модулям операционной системы. Последние последовательно передают его модулям, управляющим работой жестких дисков или флеш–носителей. Затем на диске возникает файл, содержащий набранный текст. Данные пояснения необходимы для формулирования понятия потоков информации, реализующих процессы в рамках цифровой платформы.

Как мы покажем ниже, не любая компьютерная система является цифровой платформой, но СО-модель позволяет сформулировать и обосновать свойства, необходимые для того, чтобы считать КС платформой.

СВОЙСТВА ПОТОКОВ ИНФОРМАЦИИ В ЦИФРОВОЙ ПЛАТФОРМЕ

Потоки внутри платформы имеют следующие особенности, определяемые свойствами и назначением субъектов и объектов.

Процесс передачи информации от одного объекта к другому (обмена информацией между участниками платформы, либо ее перемещения от участника в хранилище информации, либо обратно направленного перемещения информации) называется «потоком данных» и происходит по инициативе субъекта.

Изменение существующих и порождение новых объектов в цифровой платформе производится субъектами, т.е. программами (активными компонентами), управляемыми участниками ЦП. При этом субъекты порождают потоки информации, а также влияют друг на друга через изменяемые ими объекты.

Как мы указывали выше, субъекты и объекты отличаются друг от друга по свойству их активности. В отличие от субъекта человек–пользователь (участник) – лицо, идентифицируемое некоторой информацией, то есть представившееся используемой им компьютерной системе и управляющее субъектом КС посредством органов управления компьютером. По отношению к субъекту он является внешним фактором, определяющим его состояние.

Процедуры идентификации (ввода пользователем его имени) и аутентификации (подтверждения индивидуальности участника платформы паролем, аппаратным носителем, сертификатом и т.д.) применяются и для определения прав и функций участников платформы.

Цифровая платформа является распределенной компьютерной системой, в которой протекают распределенные информационные процессы. В рамках ЦП выделяется локальный сегмент (ЛС), к которому относится участник ЦП, и внешний сегмент, т.е. подмножество субъектов и объектов, к которому он не отно-

сится.

Существует несколько критериев определения локального сегмента ЦП:

- группирование всех субъектов в одно множество с возможностью непосредственного управления ими (персональное рабочее место участника платформы);
- нахождение некоторого подмножества объектов и субъектов в рамках одной технической компоненты платформы (локальная сеть организации);
- или присвоение объектам и субъектам сетевого адреса, например, mail.ru – большое количество серверов, управляющих компьютеров и каналов связи, расположенных в нескольких странах, но решающих одну задачу по хранению и доставке электронной почты.

Остальной сегмент является дополнением множества субъектов и объектов ЛС по указанным критериям до всего множества объектов и субъектов ЦП, включающего другие локальные сегменты.

Внешним субъектом мы называем субъект, принадлежащий множеству субъектов внешнего сегмента, при этом полагаем, что множества субъектов локального и внешнего сегмента не пересекаются.

Доступ внешнего субъекта к локальному объекту предполагает поток информации от внешнего объекта к объектам локального сегмента.

Поясним взаимодействие внешнего и локального сегмента (представлено на рисунке 1)

Понятие потока описывает работу компьютерной системы ЦП под управлением участника ЦП. Например, потоки во «внешний мир» соответствуют запросам во внешние относительно ЦП информационные хранилища и базы данных, обратные потоки – ответы на эти запросы. Потоки от одного ЛС ЦП к другому через внешний сегмент означают информационный обмен между участниками.

Потоком информации (англ. stream) от объекта O_m к объекту O_j называется операция над объектом O_j, реализуемая в субъекте S_i и зависящая от O_m: $Stream(S_i,O_m)\text{–>}O_j$ (рисунок 2). При этом для практической работы следует выделять источник (O_m) и получателя потока (O_j). Значения индексов принимают целые положительные значения и означают порядковый но-

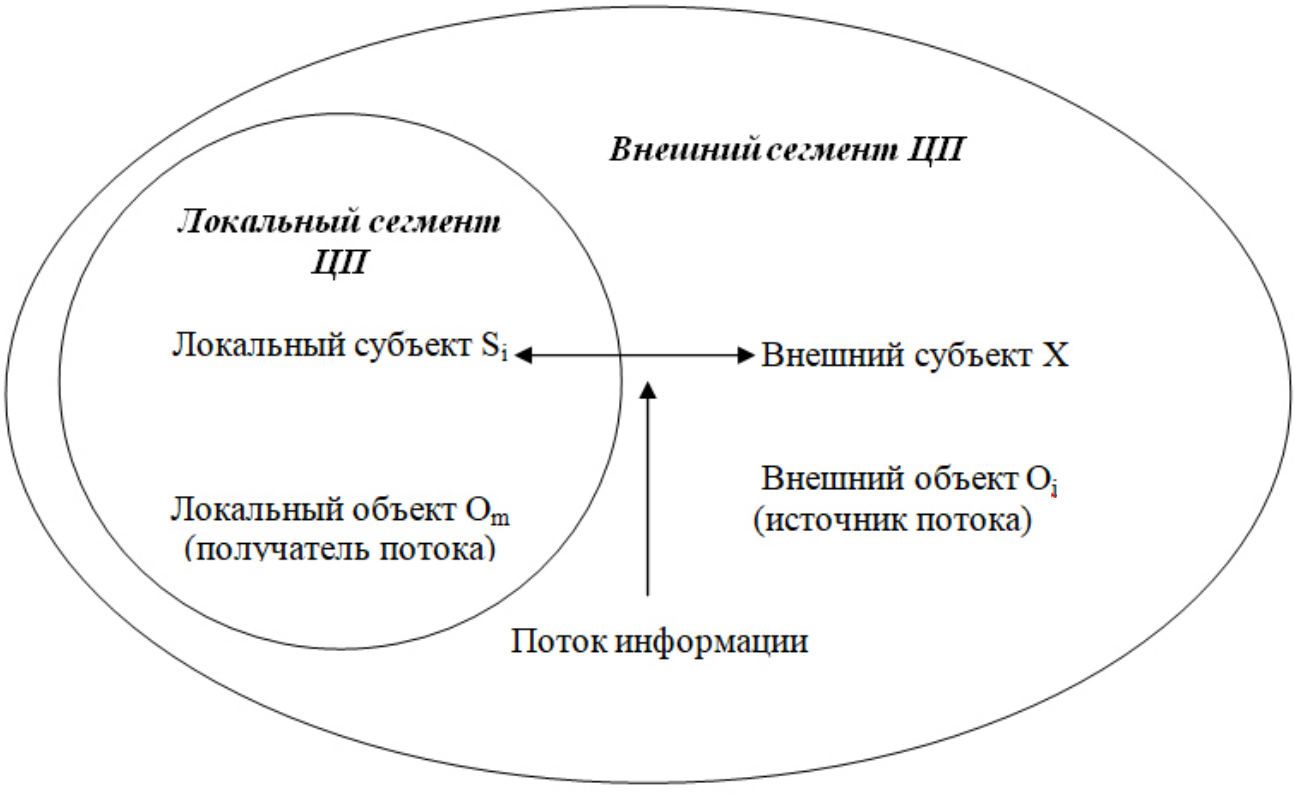

Рис. 1. Взаимодействие субъектов S_i локального и X внешнего сегмента

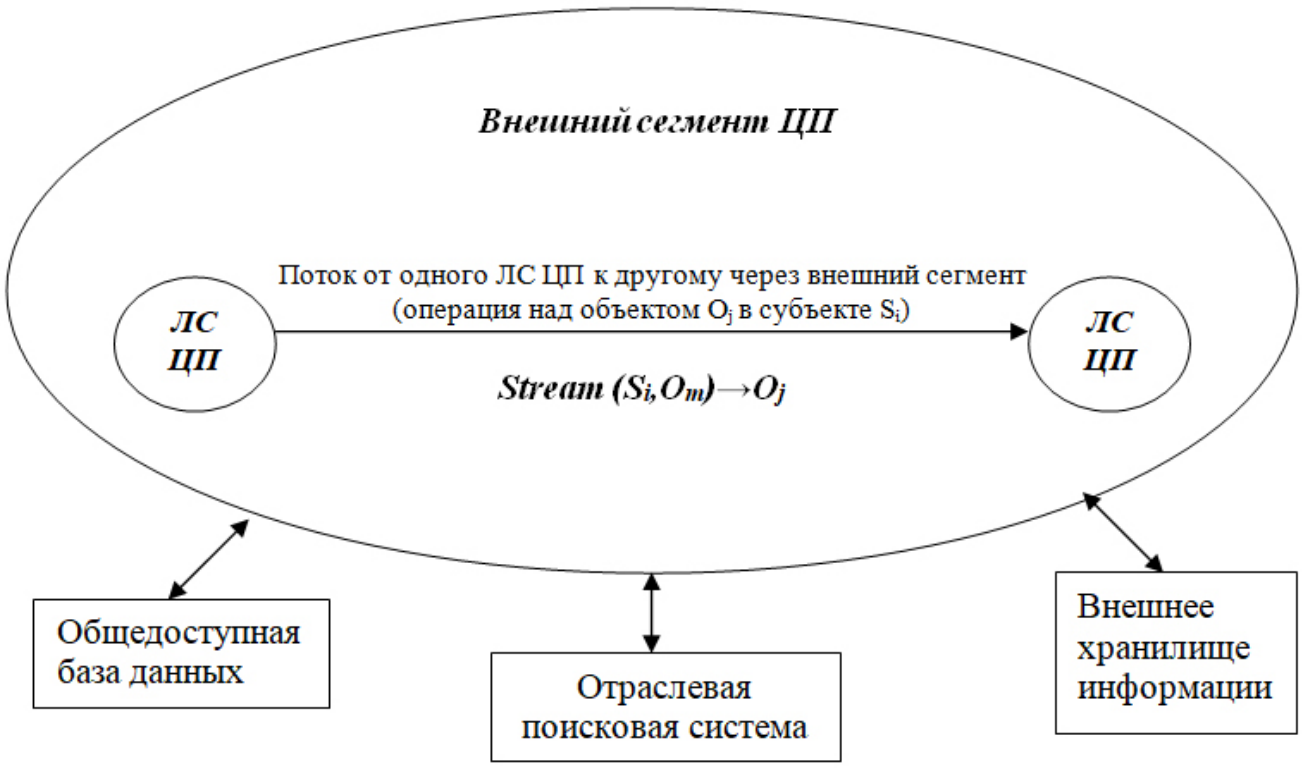

Рис. 2. Направления потоков внутри ЦП и к внешним системам

мер субъекта или объекта.

Приведенные определения и разъяснения обладают большой теоретической значимостью, поскольку они позволяют понять, как конструируются локальные сегменты ЦП, соединяющие несколько локальных систем.

Основным для передачи информации и контроля информационных потоков свойством является свойство транзитивности: если существует поток от А к В и поток от В к С, то существует и поток от А к С [1]. Поток, проходящий через несколько объектов, называется составным потоком (в данном случае - от А к С).

Наличием локального и внешнего сегментов ЦП определяется разделение множества всех потоков на следующие четыре группы (рисунок 3):

1. Потоки между локальными субъектами и локальными объектами описывают работу участника, запускающего некоторую программу, которая обрабатывает данные из ЛС ЦП на отдельном рабочем месте участника или во внутренней сети организации.

2. Потоки между локальными субъектами и внешними объектами возникают при работе участника с внешним ресурсом при помощи собственных программ, размещенных на ЛС ЦП.

3. Потоки между внешними субъектами и локальными объектами означают, что внешние субъекты пользуются внутренними ресурсами ЛС ЦП.

4. Потоки между внешними субъектами и внешними объектами означают работу внешних пользователей.

Понимание принципов функционирования разных групп потоков, дает возможность оценить, как участник ЦП может получать информацию извне, обмениваться данными внутри своей замкнутой локальной системы, не имеющей выхода во внешние ЦП, с другими локальными сегментами или внешними платформами, как к его данным может получить доступ удаленный субъект.

Рассмотрим далее операцию порождения субъекта Create(S_j,Oi)–>S_k. В данном случае из объекта Oi порожден субъект S_k под воздействием субъекта S_j.

Операция порождения субъектов описывает запуск активным субъектом исполняемого мо-

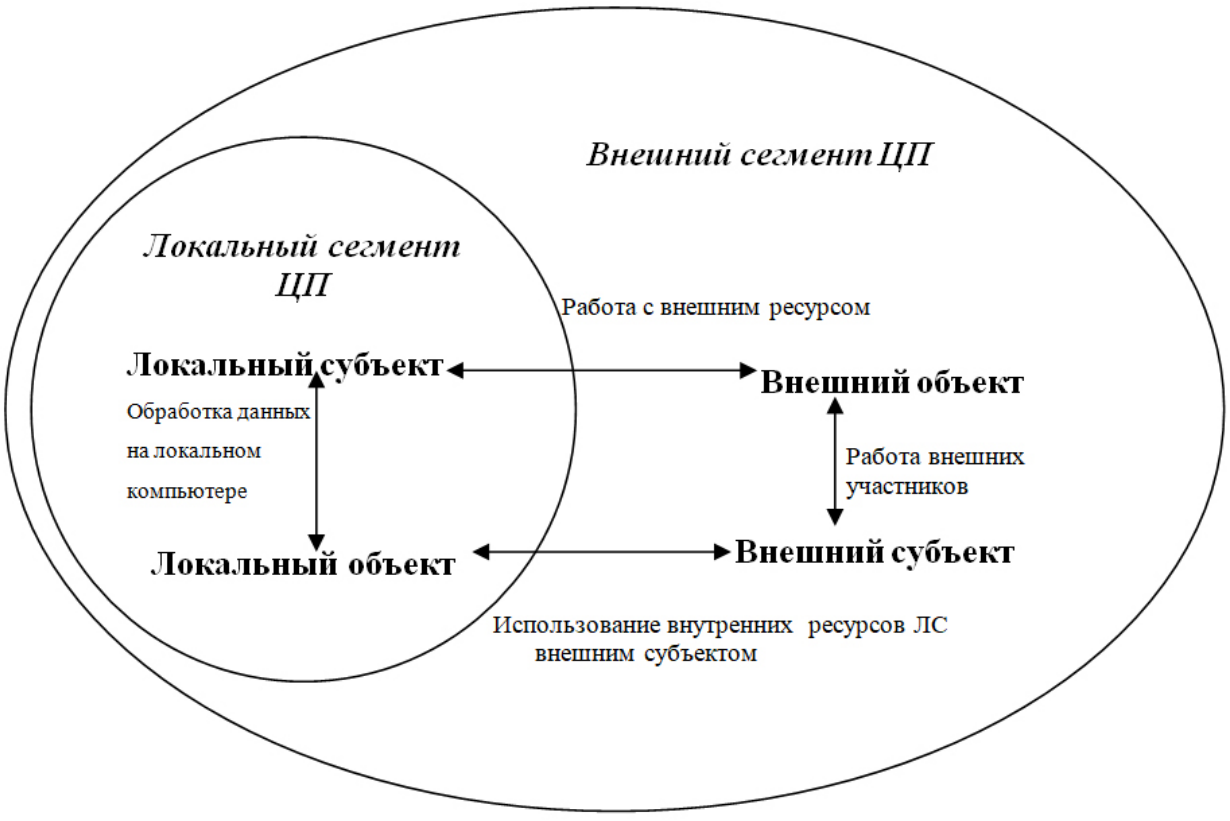

Рис. 3. Виды потоков в рамках ЦП

дуля в ЦП, после чего объект становится субъектом и начинают исполняться находящиеся в нем инструкции процессора.

У субъекта–программы есть ассо-циированные с ним объекты (поля программы, последовательность действий программы и др.), которые содержат информацию о его состоянии.

В случае взаимодействия между удаленным субъектом X и локальным субъектом S_i i-й субъект – взаимодействующая с сетью программа компьютера. Целью данного взаимодействия является реализация потока между объектом O_j локального сегмента и ассоциированным объектом O_x субъекта X внешнего сегмента ЦП через ассоциированные объекты субъекта S_i ЛС, например, при обращении во внешний сегмент ЦП через локальную программу S_i (пример локального субъекта- Internet Explorer), которая связывается с внешней программой X.

Это взаимодействие происходит как в случае «добросовестного» сетевого общения, так и при атаках внешнего нарушителя.

Однако возможна и передача из внешней сети объекта O_v, который может в результате запуска в рамках ЛС ЦП породить новый субъект в локальном сегменте.

Порождение нового субъекта может произойти из объекта, находящегося как в локальном сегменте ЦП, так и во внешнем.

Укажем следующие обозначения: X – субъект внешнего сегмента платформы, который инициирует поток через S_i – субъект, принадлежащий подмножеству субъектов ЛС ЦП; O_j – объект локального сегмента. Объекты O_j и O_k входят в множество объектов ЛС ЦП.

Допустим, упрощенная модель платформы состоит из двух компьютеров участников с установленным программным обеспечением, обеспечивающим совместную работу прикладных программ, и аппаратуры передачи данных для обмена информацией. При этом передаваемая и принимаемая информация представляется в платформе на разных уровнях (файлы и их части, пакеты).

Тогда потоки от ассоциированного объекта O_x субъекта X к ассоциированному объекту O_k субъекта S_i и наоборот описываются следующим образом: $Stream(X,O_x)–>O_k$ и $Stream(X,O_k)–>O_x$. При этом свойства субъекта S_i

таковы, что возможно существование потоков вида Stream(S_i,O_j)–>O_k и Stream(S_i,O_k)–>O_j.

Свойство транзитивности потоков, рассмотренное выше, является основой для построения как систем обмена данными между ЦП, так и подсистемы безопасности ЦП, построения подсистем семантического преобразования информации и для интеграции в рамках платформ. По свойству транзитивности потоков субъект X получает доступ к объекту O_j через субъект S_i.

В локальном сегменте ЦП возможны также две основные ситуации, связанные с упомянутой выше возможностью порождения нового субъекта:

1. Доступ к объекту O_j со стороны субъекта S_i под влиянием субъекта X. Таким образом, внешний субъект X может получить доступ к объектам локального сегмента непосредственно через телекоммуникационный субъект, через который участник «видит» внешний сегмент ЦП.

2. Порождение субъектом S_i из локального объекта нового субъекта S_i*, для которого существует поток Stream(X,S_i*).

Рассмотренные ситуации описывают модели интеграции субъектов в рамках ЦП.

Для обеспечения интеграции процессов (совокупности субъектов и их операций над объектами) в рамках модели платформ необходимо детально рассмотреть те свойства, которые позволяют квалифицировать информационную систему как платформу.

СВОЙСТВА ЦИФРОВЫХ ПЛАТФОРМ, ЗНАЧИМЫЕ ДЛЯ ИХ ИНТЕГРАЦИИ

В исходных понятиях ЦП и СО-модели уже предполагаются свойства интегративности (способности объединять две или множество частей в единое органично функционирующее целое) и развития (способности позитивно влиять на развитие элементов системы в результате синергии их взаимодействия).

Понятие платформы, появившееся после перехода коммуникаций в цифровую плоскость, означает в первичном узком смысле сочетание аппаратного и связующего программного обеспечения (операционной системы) персонального компьютера, необходимое для воспроизведения прикладных программ, или аппаратно-программный комплекс с базовым набором сервисов, выполняющих определённые задачи. Кроме того, платформы выделяют также по отдельным функциональным признакам, в таком случае они составляют основу для обеспечения функций какими-либо субъектами (передача данных для транспортной платформы, управление сетью для административной платформы, исполнение программного кода для процессора и др.) [4].

В широком смысле под термином «платформа» в настоящее время понимается совокупность технологий (на основе которых реализуются процессы и приложения), служащих механизмом объединения усилий всех заинтересованных в решении конкретных задач сторон. Данное определение нужно иметь в виду при построении отраслевых цифровых платформ.

Анализ базовых свойств платформ необходим для внедрения их как инструментов организации работы сложных систем, включающих участников разнонаправленных информационных процессов, управляющих субъектами информационной системы с целью эффективного выполнения задач их функциональной деятельности. От соответствия ЦП требованиям к их свойствам напрямую зависит уровень и темпы развития научно-технического развития экономики и общества в целом.

Поскольку цифровые платформы относятся к информационным системам, следует прежде всего обратиться к основным понятиям информационных систем.

В соответствии с международным стандартом ISO/IEC 2382:2015 [5] информационная система - это система обработки информации и связанные с ней человеческие и технические ресурсы. ИС содержит подсистемы, состоящие, например, из персональных ЭВМ, периферийных устройств и программного обеспечения для обработки данных, и включает в т.ч. компьютерную систему в соответствии с [1].

Напомним, что мы рассматриваем как информационную, так и компьютерную систему в рамках субъектно-объектной модели, как совокупность активных сущностей – субъектов

и объектов, с которыми оперируют субъекты, управляемые участниками ЦП.

Для построения цифровой платформы в узком смысле важно соответствие требованиям высокой производительности, отказоустойчивости, надежности и масштабируемости.

На сегодняшний день однородные сети программно совместимых компьютеров постепенно вытесняются неоднородными сетями, объединяющими компьютеры разных производителей (распределенным многозадачным мультиресурсным системам), что приводит к появлению новых требований. Последние касаются прежде всего возможности использования нового аппаратного и программного обеспечения в соответствии с новыми требованиями и решаемыми задачами на прежней аппаратной платформе, обеспечения мобильности программ (работы программных средств на разных платформах), применения единых интерфейсов на всех компонентах.

В соответствии с описанными тенденциями данные свойства являются необходимыми условиями корректного функционирования информационной системы.

Для определения основных закономерностей процессов интеграции укажем с учетом основных свойств систем, сформулированных в рамках системного анализа [6], следующие свойства и требования к информационной системе, соответствие которым позволяет оценить ее как цифровую платформу в широком смысле слова, далее определим влияние СО-модели, и, в частности, процессов потоков и порождений на интегрируемость платформ (место СО-модели в концепции платформ):

1. Масштабируемость - свойство (или способность) информационной системы обрабатывать растущий объем задач таким образом, чтобы дополнительные ресурсы (вычислительные возможности, новые функциональные элементы, выполняющие сходные задачи), соответствовали приросту производительности [7]. Таким образом, система при помощи средств распределения вычислений и данных, может включать новых участников или увеличивать объем обрабатываемых данных, поддерживая требуемый уровень производительности. Пример: масштабируемая поисковая система продолжает корректно обрабатывать запросы при увеличении числа пользователей и индексируемых объектов.

Масштабируемость цифровой платформы напрямую следует из базовых свойств СО-модели, в первую очередь – возможности порождения необходимых процессов в количестве, требуемом для поддержания масштаба платформы и обеспечения распределенных вычислений.

2. Тиражируемость платформы – возможность ее адаптации и внедрения в других условиях без изменения структуры и состава субъектов. Неизменность типовых свойств создает условия для дальнейшей интеграции. Тиражируемость определяется возможностью типизации входящих в платформу объектов, причем как объектов-данных, так и объектов-источников для порождения субъектов.

3. Расширяемость – свойство, связанное с дополнением субъектов, реализующих новые функции, с сохранением неизменности структуры и потоков данных. Расширяемость является с точки зрения СО-модели одним из важнейших свойств ЦП, обеспечивающим включение в ЦП новых субъектов, за счет которых платформа приобретает новые свойства, позволяющие развивать и интегрировать цифровые платформы. Таким образом, расширяемость как возможность включения в ЦП новых субъектов является необходимым и диалектически неотъемлемым для платформ условием развития.

4. Развитие – свойство системы сохранять и приобретать новые качества (наращивать потенциал) на всех этапах жизненного цикла. Свойство развития проявляется, в частности, при переходе из количественных характеристик в качественные в области обработки больших данных. Необходимым условием развития является включенность в ЦП средств разработки информационного и программного обеспечения.

5. Замкнутость связана с фиксированным количеством субъектов в текущий момент времени. Данное свойство необходимо на этапе эксплуатации ЦП (напомним, что жизненный цикл цифровой платформы включает этапы разработки, реализации, эксплуатации, сопровождения, модификации и вывода из эксплуатации).

Замкнутость позволяет обеспечить сопровождаемость процессов в ЦП, то есть возможность установить по цепочкам порождений субъектов и потокам данных, где именно возникают ошибочные ситуации в ЦП. Кроме того, замкнутость позволяет управлять процессами информационной безопасности ЦП, поскольку незамкнутая система является принципиально незащищенной.

6. Целостность – свойство, связанное со способностью системы сохранять внутреннюю логику и структуру в процессе решения задач, которые не могут быть решены отдельными компонентами системы. Целостность с точки зрения СО-модели обеспечивает стабильность работы ЦП: из одних и тех же объектов-источников порождаются одни и те же субъекты.

7. Безопасность – свойство, связанное с целостностью и замкнутостью, к которому дополнены свойства конфиденциальности и доступности. Свойство безопасности мы уже прокомментировали и обосновали выше.

8. Возможность связи платформ между собой, в первую очередь за счет наличия единых или стандартизированных интерфейсов. Связь платформ между собой гарантируется определяемыми СО-моделью свойствами транзитивности потоков и существования составного потока между элементами ЦП. Без данных свойств СО-модели недостижима интеграция цифровых платформ.

ВЫВОДЫ

Субъектно-объектная модель КС позволяет с одной стороны выявить и обосновать необходимые свойства, которые позволяют считать компьютерную систему платформой, а с другой – конструктивно применима для описания платформенных решений и для интеграции цифровых платформ между собой в первую очередь за счет транзитивности потоков информации. Возможность обеспечения ЦП средствами распределения вычислений и данных, а также требуемого количества процессов при увеличении количества субъектов ЦП с новыми функциями позволяет сохранять и увеличивать производительность цифровой платформы и является необходимым и диалектически неотъемлемым условием ее развития и интеграции с иными платформами.

СПИСОК ЛИТЕРАТУРЫ

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты // Учебное пособие. – М.: Книжный мир, 2009. – 352 с.

2. Aspray W. John von Neumann and the Origins of Modern Computing. — MIT Press, 1990. – 394 p.

3. Рязанова А.А. Цифровые платформы: интегративный потенциал, основные понятия и свойства // Вестник современных цифровых технологий. 2020. № 4. С. 28-39.

4. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е изд. – СПб.: Питер, 2013. – 816 с.

5. ISO/IEC 2382:2015(en) Information technology – Vocabulary [Электронный ресурс] // Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

6. Ракитов А.И., Бондяев Д.А., Романов И.Б., Егерев С.В., Щербаков А.Ю. Системный анализ и аналитические исследования: руководство для профессиональных аналитиков // Типография «Возрождение», 2009. – 448 с.

7. Bondi André B. Characteristics of scalability and their impact on performance // Proceedings of the second international workshop on Software and performance – WOSP '00. – P. 195. doi:10.1145/350391.350432.

УДК: 336.1, 336.7, 004.056

Принципы создания прототипа универсальной цифровой монеты

S.A. Borodulina, I.A. Selionov, A.A. Tyumentsev, P.A. Cherkashin, A.Yu. Shcherbakov

Principles for Creating a Prototype of a Universal Digital Coin

Abstract. *The article discusses the concept of digital coins as a means of achieving independence and mobility of the national financial system, reducing the cost of paper money circulation, strengthening the economic security of the state. The necessity of using symmetric cryptography mechanisms and rejection of certification centers is shown. The preliminary structure of a digital coin is given. A brief description of the system and technology of circulation of digital coins is presented.*

Keywords: *digital coin, zero processing, asymmetric cryptography, national credit institution, national central bank.*

С.А. Бородулина[1]
И.А. Селионов[2]
А.А. Тюменцев[3]
П.А.Черкашин[4]
А.Ю. Щербаков[5]
[1]Председатель правления Ассоциации «Евразийский деловой совет»
E-mail:info@eurasia.business
[2]Директор по стратегическому развитию управляющей компании "Технопарк Пушкино", вице-президент РАКИБ
E-mail: uk04@inbox.ru
[3]Генеральный директор ООО «Тюменцев и партнеры».
E-mail: tyumentsev@mail.ru
[4]Научный сотрудник Ассоциации РКЦФА
E-mail: pcherkashin@gmail.com
[5]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *В статье рассматривается концепция цифровых монет в качестве средства достижения независимости и мобильности национальной финансовой системы, снижения издержек на бумажное денежное обращение, укрепления экономической безопасности государства. Показана необходимость использования механизмов симметричной криптографии и отказа от удостоверяющих центров. Приведена предварительная структура цифровой монеты. Представлено краткое описание системы и технологии обращения цифровых монет.*

Ключевые слова: *цифровая монета, нулевой процессинг, асимметричная криптография, национальная кредитная организация, национальный центральный банк.*

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ

В современной экономической и геополитической ситуации намечаются тенденции центробежного характера, связанные со стремлением государств с их национальными денежными и финансовыми системами к выходу из общемировой системы денежного оборота, привязанного к доллару.

С другой стороны, развитие финансовой системы происходит в сторону снижения стоимости обслуживания наличного денежного оборота за счет внедрения безналичных платежных инструментов (например, пластиковых карт). При этом часто не учитывается ситуация, связанная с тем, что процессинг пластиковых карт выполняется теми же транснациональными финансовыми корпорациями, что существенно снижает независимость и мобильность национальной финансовой системы.

Учитывая описанные тенденции, можно констатировать, что для создания устойчивого к внешнему влиянию денежного обращения, свободного также и от сложностей и издержек бумажного денежного оборота, необходима разработка концепции и методологии цифровых монет.

Важно заметить, что движение цифровых монет решает задачу контроля денежного обращения с точки зрения борьбы с отмыванием доходов, полученных преступным путем, и ряд других вопросов, связанных с экономической безопасностью государства.

ИСХОДНЫЕ ПОЛОЖЕНИЯ ПРОЕКТА

Вполне очевидно, что для цифровой монеты, рассматриваемой как материальный объект определенной структуры, циркулирующий в общедоступных сетях передачи данных, в обязательном порядке необходимо использование криптографических механизмов при эмиссии (фиксация номинала и серии-номера монеты) и при движении (проверка валидности при переводах и торговых операциях).

При этом применение механизмов электронной подписи, особенно квалифицированной, использующей удостоверяющие центры для массового движения цифровых монет (ЦМ), попросту невозможно, поскольку утяжелит систему и, в частности, из-за проблемы отозванных сертификатов сделает невозможной ее эксплуатацию, вплоть до полной остановки системы. Кроме того, использование асимметричных алгоритмов также сделает систему неработоспособной. Это относится и к процедурам реализации «слепой подписи» для ЦМ [1].

Вполне очевидно, что хранилищами ЦМ и средствами их распоряжения могут стать массово используемые мобильные устройства (мобильные телефоны) клиентов. Однако реализация криптографических механизмов в рамках личного мобильного устройства сопряжена с рядом проблем как технического, так нормативного характера. В связи с этим наличие криптографических механизмов на кошельках клиентов требуется минимизировать, а в идеальном случае – исключить.

ОСНОВНАЯ ИДЕЯ ПРОЕКТА

Основной идеей проекта ЦМ является использование механизмов симметричной криптографии и качественных датчиков случайных чисел для генерации отдельных ЦМ с уникальным номером и последующее хранение эмитированных монет в национальном центральном банке, либо уполномоченной (аккредитованной) им службе процессинга.

При этом должна быть обеспечена невозможность компрометации системы при компрометации или утрате любого количества кошельков пользователей.

Кроме того, должно быть обеспечено неиспользование удостоверяющих центров.

Будем полагать, что система движения ЦМ состоит из нескольких национальных финансовых регуляторов (национальных центральных банков - НЦБ), подчиненных им национальных кредитных организаций (НКО) и клиентов. При этом данная иерархическая структура позволит заложить в систему ЦМ и трансграничные свойства – движение монет между НЦБ через общий «нулевой процессинг». По сравнению с базовой статьей [2], описывающей структуру универсального токена, предлагаемая концепция и методология движения ЦМ является принципиально новой, конструктивной и практически реализуемой.

УЧАСТНИКИ СИСТЕМЫ ОБРАЩЕНИЯ ЦИФРОВЫХ МОНЕТ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Нулевой процессинг (НП) – уполномоченная (аккредитованная) национальным ЦБ служба процессинга, хранящая ключ НК0, обеспечивающий эмиссию монет и, при необходимости, учет всех транзакций участников.

Национальный центральный банк (НЦБ) – участник системы, владелец ключа КНЦБi, создаваемого либо на стороне НЦБ, либо на стороне НП. Ключ передается в виде защищенного контейнера и используется для проверки монет, циркулирующих между НЦБ и НП.

Национальная кредитная организация (НКО) – подчиненная НЦБ структура, владелец ключа КНКОj, используемого в тракте НКО-НЦБ.

Клиент – владелец мобильного приложения, содержащего монеты и дающий распоряжения по их использованию. Клиенту создается при регистрации в НКО ключ ККm, на котором вычисляется КА монет, переданных ему. Контейнер клиента может храниться на стороне НКО и открываться по каждой операции клиента, сопровождаемой распоряжением.

Распоряжение по операции с ЦМ – выраженное и зафиксированное в приложении клиента решение о перемещении монет (совершении операций). Для распоряжения необходима

сумма и имя клиента-получателя.

В системе рассматриваются следующие операции:

- перевод ЦМ,
- покупка при помощи ЦМ,
- размен ЦМ,
- обращение к справочнику клиентов.

Клиенты в системе имеют имя и соответствующий ему номер мобильного устройства. Один клиент может иметь несколько имен.

Код аутентификации (КА) – результат работы процедуры вычисления значения, зависящего от значения ключа и содержания информации. Эта процедура такова, что без знания ключа невозможно или вычислительно трудоемко рассчитать КА к заданной информации [3].

ПРЕДВАРИТЕЛЬНАЯ СТРУКТУРА ЦИФРОВОЙ МОНЕТЫ

Таблица 1

Предварительная структура цифровой монеты

№№	Назначение поля	Длина, байт	Примечание
1	Заголовок	8	
2	Идентификатор криптоалгоритма	2	
3	Номинал	4	
4	Номинал дробный	4	Зарезервировано, в данном проекте не используется
5	Серия, номер монеты	16	
6	Дата-время выпуска монеты	8	
7	Срок жизни монеты, до…	8	
8	Имя НЦБ	16	
9	Имя НКО	16	
10	Имя клиента	16	
11	Время последней транзакции	8	
12	Порядковый номер последней транзакции	8	Приращивается к предыдущему значению поля; обслуживание монеты с меньшим номером исключено
13	Статус монеты	2	Активна/неактивна
14	Резерв	8	Заполняется нулями
15	Код аутентификации (КА) НП на поля 1-13	8	Вычисляется на секретном ключе К0
16	Код аутентификации (КА) НЦБ на поля 1-13	8	Вычисляется на секретном ключе КНЦБi
17	Код аутентификации (КА) НКО на поля 1-13	8	Вычисляется на секретном ключе КНКОj
18	Код аутентификации (КА) клиента на поля 1-13	8	Вычисляется на секретном ключе ККm
19	Резервное поле	32	
	ИТОГО	186	

КРАТКОЕ ОПИСАНИЕ ТЕХНОЛОГИИ ДВИЖЕНИЯ ЦИФРОВОЙ МОНЕТЫ

1. НП эмитирует необходимое количество монет и фиксирует их КА на секретном ключе К0. НП регистрирует в системе НЦБ и формирует, либо получает от НЦБ ключ КНЦБi.

2. Передача НЦБ сформированного пула монет. НЦБ добавляет к каждой монете КА НЦБ.

3. НЦБ регистрирует ЦМ в системе НКО, формируя ключи КНКОj.

НЦБ инкассирует в НКО монеты и формирует в них КА НКО. НКО при получении проверяют КА НЦБ.

4. НКО подключает пользователей путем регистрации их приложений (кошельков) и формирования имен для них, и загружает в кошельки (или на карты) монеты с вычислением КА владельца на ККm.

5. При покупке или переводе файл монеты переходит к другому владельцу и в кошельке первичного владельца уничтожается. При этом увеличивается счетчик транзакций и меняется время последней транзакции. По всей цепочке передачи КА проверяются и при движении к новому владельцу пересчитываются на соответствующих ключах с изменением имен (НЦБ при трансграничной передаче, НКО при передаче в другую НКО, либо клиента - при передаче в рамках одной НКО, либо все необходимые поля).

6. При онлайн-платежах информация синхронно обновляется в базе НП и НЦБ, при офлайн-платежах информация остается в НКО или кассе и синхронизируется после завершения операционного дня, либо снятия кассы, либо периодически при большом числе транзакций. При этом поле статуса неактивно до подтверждения монеты в НП.

7. Если клиент не может подобрать сумму из имеющихся у него монет, он запрашивает процедуру размена монет – перечисляет монету в НЦБ и получает несколько монет, равных сумме отправленной (с вычислением всех КА при движении ЦМ).

8. Для перевода или покупки клиент или НКО может запросить имя абонента по номеру его телефона, используя справочники НКО и клиентов, размещенных в НЦБ.

9. Монеты могут быть выгружены в «холодные» кошельки (флеш-носитель), либо распечатаны в бумажном виде с визуализацией указанных выше полей в цифровом виде, либо в виде двумерного кода. При этом возможно предъявить «бумажную» ЦМ, которая будет загружена в систему. В дальнейшем она будет циркулировать цифровом виде.

Предложенная система может показаться излишне централизованной, поскольку требуется проверка или пересчет КА в каждом ее звене. Однако это увеличивает защищенность движения ЦМ и позволяет вести их полный учет. Кроме того, алгоритмы расчета КА в настоящее время являются весьма быстродействующими, а малый размер ЦМ не перегрузит современные каналы связи.

В ряде случаев возможна передача клиенту ЦМ в виде смс-сообщения.

Таким образом, при расчете КА для клиента в рамках национальной кредитной организации и последующей его проверке в той же или другой НКО, входящей в централизованную систему с нулевым процессингом, возможно использование цифровых монет в рамках других национальных центральных банков, подключенных к системе (трансграничные расчеты и оборот). При этом не требуется реализация криптографических механизмов в кошельке клиента.

ВЫВОДЫ

Предлагаемая концепция может стать основой для создания независимой системы цифрового денежного обращения для снижения влияния международного экономического санкционного фона, а при наличии нескольких связанных общим процессингом НЦБ – обеспечить доверенные и независимые трансграничные платежи и повысить устойчивость национальных экономик.

Подводя итоги, можно назвать следующие принципиальные преимущества цифровой монеты:

- высокая степень защиты от подделки и возможность автоматического восстановления при помощи вычисления КА;

- трекинг движения средств и возможность прослеживания нахождения каждой монеты;
- существенное снижение затрат на обслуживание бумажных денег;
- возможность перевода монеты в бумажную форму и обратно;
- оптимизация социальных выплат и выплат дивидендов;
- возможность оперативного регулирования денежной массы в рамках национальной экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Слепая подпись. URL: https://ru.wikipedia.org/wiki/Слепая_подпись (дата обращения: 12.04.2021).
2. Гриняев С.Н., Злотин Р.А., Милушкин А.И., Правиков Д.И., Селионов И.А., Щербаков А.Ю., Щуко Ю.Н. К вопросу о создании универсального защищенного доверенного цифрового актива (токена) // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационный процессы и системы. 2018. № 10. С. 20-28.
3. Код аутентификации. URL: https://dic.academic.ru/dic.nsf/fin_enc/23875 (дата обращения: 12.04.2021).

УДК: 004.3, 004.9

Концепция информационной безопасности «роя» киберфизических систем

D.I. Pravikov, A.Yu. Shcherbakov

The Concept of Information Security of the "Swarm" of Cyber-Physical Systems

Abstract. *The article is devoted to consideration of possible approaches to ensuring information security, taking into account the peculiarities of cyber-physical systems in theoretical and practical aspects. The issues of information security assurance of a set of cyber-physical devices operating in the absence of a "secure perimeter" are considered. A solution to these issues is proposed by including the functions of forming an "intelligent swarm" with distributed mechanisms for ensuring information security in cyber-physical devices. An algorithm for ensuring information security of a "swarm" of cyber-physical devices is described.*

Keywords: *cyber-physical system, insecure environment, information security of the swarm, application environment descriptor, distributed ledger, man-in-the-middle attack, subject-object model.*

Д.И. Правиков[1]
А.Ю. Щербаков[2]
[1]Кандидат технических наук, руководитель Научно-образовательного центра новых информационно-аналитических технологий РГУ нефти и газа (НИУ) имени И.М. Губкина
E-mail: dip@gubkin.pro
[2]Доктор технических наук, начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена рассмотрению возможных подходов к обеспечению информационной безопасности, учитывающих особенности киберфизических систем в теоретическом и практическом аспектах. Рассмотрены вопросы обеспечения информационной безопасности набора киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра». Предложено решение данных вопросов при помощи включения функций формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности, в киберфизических устройствах. Описан алгоритм обеспечения информационной безопасности «роя» киберфизических устройств.*

Ключевые слова: *киберфизическая система, незащищенная среда, информационная безопасность «роя», дескриптор прикладной среды, распределенный реестр, атака «человек посередине», субъектно-объектная модель.*

ВВЕДЕНИЕ

В настоящее время теория информационной безопасности находится в состоянии, которое можно охарактеризовать как приближение к точке бифуркации. С одной стороны существует уже общепризнанная теория, базирующаяся на субъектно-объектной модели, которая в основном используется для «традиционных» автоматизированных информационных систем. С другой стороны, резкое развитие киберфизических систем (КФС) и применение их для решения ряда задач привели к появлению запроса на формирование новых подходов к обеспечению информационной безопасности, учитывающих особенности КФС как в теоретическом, так и практическом плане.

Так, например, специалисты в области обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) в ряде работ и в выступлениях на конференциях отмечают исчезновение «периметра» - одного из базовых постулатов классической теории информационной безопасности. Как следствие, для ряда случаев уже не применимо понятие «контролируемой зоны», а значит защищаемые элементы, в роли которых выступают киберфизические системы, должны функционировать фактически в незащищенной среде, тем не менее, обеспечивая заданные свойства безопасности. Эти проблемы в полной мере относятся и к системам обращения цифровых активов, блокчейн-платформам, платежным системам, которые корректно рассматривать только как комплексные киберфизические системы.

На текущий момент трудно судить как о наличии теории обеспечения информационной безопасности КФС, так и об общепризнанных подходах к ее формированию. Рассмотрению возможных подходов к решению указанных

проблем посвящена данная работа.

АНАЛИЗ

Обеспечение информационной безопасности киберфизических систем (как комплексов киберфизических устройств), является предметом изучения различных научных коллективов. Достаточно упомянуть работу [1]. При этом можно утверждать, что, несмотря на предпринимаемые усилия, в настоящее время не существует теории, позволяющей смоделировать и формализовать аспекты информационной безопасности комплекса киберфизических устройств. Современные тенденции, идущие от практики, связаны с появлением таких подходов, как архитектура «с нулевым доверием»[1], для которой существуют решения по обеспечению безопасности. Однако эти подходы не имеют соответствующего теоретического обоснования.

Такая постановка вопроса о безопасности комплекса киберфизических устройств имеет следующее объяснение.

Разработанные ранее теоретические положения и подходы опирались на постулат замкнутости защищаемой системы [2]. В субъектно-объектной модели определены и перечислены все пассивные сущности (объекты) и активные сущности (субъекты), права доступа и правила продукции (устанавливают, что произойдет, если некоторый субъект произведет разрешенное действие с некоторым объектом). Для систем подобного типа вводилась роль администратора, который фактически должен был контролировать перечни субъектов и объектов, а также задавать права доступа и полномочия.

В упомянутой выше работе [2] вводились две аксиомы защищенных компьютерных систем (КС):

Аксиома 1. В защищенной КС всегда присутствует активная компонента (субъект), выполняющая контроль операций субъектов над объектами. Данная компонента фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной КС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

Гипотетически комплекс, состоящий из киберфизических устройств, также можно было бы рассматривать как некоторую систему, состав которой зафиксирован, а безопасность обеспечивается в рамках субъекто-объектной модели. Вместе с тем, возникает проблема реализации аксиом 1 и 2 для комплексов киберфизических устройств.

Анализ различных источников показал, что одно из возможных решений было положено в основу изобретения [3], в соответствии с которым в одноранговых коммуникационных сетях киберфизических устройств осуществляется управление настройками маршрутизации, дополнительно вводится блок осуществления политики безопасности; в данном блоке «формируют правила политики безопасности в виде матрицы доступа между киберфизическими устройствами, получают запросы на сетевой доступ между киберфизическими устройствами, формируют и пересылают киберфизическим устройствам управляющие команды, внося изменения в их таблицы маршрутизации и тем самым определяя разрешенные правилами политики безопасности маршруты пересылки пакетов от одного устройства к другому».

Вместе с тем, предложенное изобретение имеет следующие ограничения:

1. Оно порождает новый объект атаки – блок осуществления политики безопасности, в отношении информационной безопасности которого в изобретении отсутствуют предложения.

2. Оно применимо для киберфизических устройств, реализующих только один прикладной процесс, т.к. приравнивает информационный обмен между киберфизическими устройствами к обмену между программами. Для киберфизических устройств с набором прикладных процессов подход, описанный в изобретении, не применим.

3. Не исключено, что при значительном количестве киберфизических устройств (де-

[1] NIST Special Publication 800-207. Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207

сятки и сотни) сложность администрирования возрастает в степенной зависимости, что делает управление безопасностью неподконтрольным на уровне возможностей обычного человека.

Более того, если мы будем рассматривать вопрос реализации указанных аксиом для комплексов киберфизических устройств, возникает вопрос, где будет располагаться компонента, выполняющая контроль субъектов над объектами и, соответственно, где и в каком виде будет размещаться информация, описывающая разрешенные операции субъектов над объектами, при условии того, что сами киберфизические устройства могут динамически как включаться комплекс, так и исключаться из него.

Рассмотрим киберфизическое устройство, функционирующее в составе комплекса других аналогичных устройств. Оно имеет подключение к локальной вычислительной сети и, в соответствии с проектом цифровизации функционального процесса, в общем случае на вход получает сигналы (управления и данных), выходом устройства также являются сигналы, которые также подразделить на данные (снимаемые с датчиков) и результаты обработки информации, полученные в результате вычислений.

В работе [4] предложена графовая модель функционирования промышленной системы (ПС), которую можно рассматривать как один из вариантов представления комплекса киберфизических устройств. Данная модель описывает сетевую инфраструктуру ПС в виде ориентированного графа G, множество вершин $V = \{v_1, \dots, v_N\}$ которого характеризует все компоненты ПС, способные к сетевому взаимодействию. Множество дуг $E = \{e_1, \dots, e_M\}$ графа отражает все возможные межкомпонентные связи, проявляющиеся как обмен данными между устройствами. Каждый компонент ПС, моделируемый вершиной v_i, характеризуется набором функций, которые он способен реализовывать:

$$f_{v_i} = \left\{ f_{v_i}^{(1)}, f_{v_i}^{(2)}, \dots, f_{v_i}^{(k)} \right\}.$$

Модель отражает взаимодействие компонентов ПС друг с другом, процессы, необходимые для реализации целевой функции ПС, и саму целевую функцию. Целевая функция F ПС представляется в модели двумя способами одновременно: в виде множества маршрутов на графе и в виде набора функциональных последовательностей с заданными типами отношений между функциями: $F = \{F_1, F_2, \dots, F_n\}$.

Данную модель можно интерпретировать следующим образом. Вершины описывают киберфизические устройства, функция f – это прикладная программа, функционирующая на киберфизическом устройстве. Соответственно дуги моделируют связи, которые, с одной стороны, возникают между киберфизическими устройствами, но в детализации описывают взаимодействие прикладных программ.

Упомянутая работа [4] интересна тем, что компьютерные атаки описаны в виде преобразований графа G. Они разделяются на структурные, представляющие собой унарные операции над G, и функциональные, заключающиеся в изменении параметров вершин и дуг.

Представленная графовая модель отражает все типы компьютерных атак на систему.

Полное перечисление возможных видов атак на промышленную систему представлено в работе [5]. Данная работа интересна тем, что на основании описания представленных видов атак, их все можно свести к набору элементарных действий:

1. Удалить информационный обмен между двумя прикладными программами (где он был).
2. Создать информационный обмен между двумя прикладными программами (где его не было).
3. Добавить новую прикладную программу (без информационного обмена).
4. Удалить существующую прикладную программу (вне зависимости от ее участия в информационном обмене).
5. Добавить новую прикладную программу и организовать ее информационный обмен с двумя другими существующими прикладными программами (комбинация действий 1, 2 и 3).

Таким образом, на основании проведенного обзора литературы можно сделать вывод о том, что информационная безопасность киберфизических устройств является предметом исследований. Поскольку функционал киберфизических устройств фактически определяется загруженным прикладным программным обе-

спечением, информационную безопасность системы киберфизических устройств можно свести к обеспечению информационной безопасности взаимодействия прикладных программ. Как следствие, само киберфизическое устройство, включая его системное программное обеспечение, должно обеспечить требуемые функции безопасности.

ИССЛЕДОВАНИЕ

Для начала определим, что множество функций (прикладных программ) и отношения информационного обмена между ними задают ориентированный граф. Таким образом, будет осуществлен переход от самих киберфизических устройств к набору функционирующих на них прикладных программ.

Тогда (пока на неформальном уровне), пусть у нас существует комплекс киберфизических устройств, работу которого мы считаем безопасной. Для него справедливы следующие постулаты.

Постулат 1. В созданном комплексе киберфизических устройств набор прикладных программ является взаимоувязанным, что подразумевает, что выход одной прикладной программы является входом для другой. Если прикладная программа получает данные извне, то эти данные являются входными для всего комплекса. Если у данных, генерируемых программой, нет потребителя, то эти данные являются выходом всего комплекса.

Постулат 2. Любая прикладная программа, находящаяся на одном из киберфизических устройств, объединенных в комплекс, не может иметь входного потока данных, кроме как входного потока для всей системы или от другой прикладной программы, зарегистрированной в комплексе.

Постулат 3. Любая прикладная программа направляет свои данные для другой прикладной программы, зарегистрированной в комплексе, либо на выход всего комплекса, описанный и заданный извне.

Исходя из описанных постулатов, можно утверждать, что изменение комплекса киберфизических устройств, приводящее к нарушению одного из постулатов, нарушает безопасность всего комплекса.

Вместе с тем, перечисленный в работе [5] перечень элементарных действий характерен и для штатной модернизации системы. В результате, если руководствоваться только тремя постулатами, будут выявляться воздействия на систему, обнаруживаемые, условно говоря, на уровне противоаварийной защиты. Более сложным случаем является, например, атака типа Man-In-The-Middle (MiM), сходная в плане своей реализации со штатной модернизацией системы. Таким образом, задача выявления атак сводится к задаче различения администрирования от несанкционированного воздействия, при условии того, что объект, реализующий положения упомянутой аксиомы 2, должен находиться за пределами отдельного киберфизического устройства.

Решение данной задачи предлагается осуществлять на основании подхода, определяющего санкционированность или несанкционированность совершаемых действий. Действие, в том числе элементарное, считается санкционированным, если запрос на его реализацию подтверждается всеми сторонами. Применительно к рассматриваемому случаю это будет означать, что совершенное действие получило подтверждение от администратора (в роли которого может выступать автоматическая система администрирования или искусственный интеллект), а также от других киберфизических устройств, перестраивающих свой информационный обмен. В результате запрос на изменение потока данных должен получить подтверждение, выработанное на основании некоего алгоритма консенсуса. Это, в свою очередь (пока теоретически) приводит к тому, что потенциальный злоумышленник при реализации атаки MiM должен инициировать получение подтверждений уже от нескольких источников, что существенно усложняет саму атаку.

В этом случае подключение нового устройства к уже существующему комплексу планируется проводить по следующему алгоритму.

Шаг 1. Перед подключением киберфизическое устройство инициали-зируется – запускается особый режим операционной системы, который опрашивает каждую загруженную в

устройство прикладную программу на предмет ожидаемых входов и выходов. Определим данный файл как дескриптор прикладной среды, в котором для каждой программы должно быть указано, от программ с какими идентификаторами ожидаются данные и программам с какими идентификаторами данные будут передаваться.

Шаг 2. Операционная система запрашивает и получает адрес распределенного реестра (идеальный вариант – каждое устройство имеет свою копию распределенного реестра), в котором уже содержатся загруженные в него ранее дескрипторы киберфизических устройств, описывающие наборы прикладных программ. Дескриптор прикладной среды выгружается в формате отдельных записей, каждая из которых описывает отдельную прикладную программу.

Шаг 3. Каждое из киберфизических устройств на основании размещения дескриптора нового устройства принимает решение о переключении информационных потоков.

Необходимо отметить, что приведенные три шага не означают реализации управления информационными потоками на технологии распределенного реестра. Исходя из попыток, описанных, в частности, в [6], создание полноценного распределенного реестра с механизмами, ориентированными на обработку криптовалют, нецелесообразно. Вместе с тем, доступно использование таких возможностей, как связанное хранение данных, когда структура данных и алгоритмы контроля целостности не допускают изменения содержания данных и их последовательности, или алгоритмы обеспечения консенсуса.

Предположим, есть Алиса, есть Боб, включается третье устройство (и это не должно реализовывать атаку «человек посредине»).

Третье устройство говорит, что у него есть программа **c**, которая готова принимать данные от программы **a** (такая есть у Алисы), а посылать –программе **b** (такая программа есть у Боба).

В дескрипторе прикладной среды описание входов и выходов каждой прикладной программы должно быть подписано администратором всего комплекса. В данном случае термин «подписано» апеллирует к возможности проверки авторства и сохранения неизменности описания входов и выходов. Важно отметить, что в киберфизической среде нецелесообразно использовать механизмы электронной подписи в их классическом варианте, достаточно ограничиться симметричными алгоритмами на основе вычисления и проверки имитовставок (модель угроз: администратор может контролировать набор прикладных программ с определенной точностью, не просчитывая возможные коллизии и ситуации, связанные с нарушением безопасности).

Тогда устройство Алисы получает дескриптор программной среды, считывает запрос, подписанный администратором приоритетным, и меняет свой дескриптор среды, отменяя передачу данных от программы **a** Бобу на передачу данных программе **c**. Боб, получая свою копию программной среды, также считывает запрос, подписанный администратором, и меняет уже свой дескриптор среды, отменяя получение данных от Алисы и меняя его на программу **c**. Тогда в блоке реестра должны появиться записи, отменяющие обмен Алисы и Боба и реализующие его через прикладную программу **c** на вновь подключаемом устройстве.

Данный блок записей реестра должен быть подписан не только Алисой, Бобом, новым устройством, но и администратором системы.

Может возникнуть вопрос, каким образом Алиса и Боб понимают, что запись в реестр осуществляет администратор, а не злоумышленник? Ответ на этот вопрос также может быть сведен к алгоритму достижения консенсуса. Так, один из алгоритмов может быть основан на Proof-of-Stake. Говоря другими словами, за администратора системы признается такая активная сущность, которая либо больше всех в течение заданного промежутка времени администрировала систему, либо получила право (подтвержденное криптографической процедурой или также консенсусом) на администрирование от той, которая больше всех администрировала систему.

Таким образом, приведенный выше алгоритм может обеспечить информационную безопасность «роя» киберфизических устройств за счет:

1. Сведения вопросов информационной

безопасности к вопросам безопасного взаимодействия и модификации набора прикладного программного обеспечения, функционирующего в комплексе киберфизических устройств (аналога субъектно-объектной модели).

2. Вынесение описания прав и порядка взаимодействия прикладного программного обеспечения (аналога таблицы разграничения прав доступа) в распределенный реестр.

3. Администрирование распределенного реестра на основании алгоритма консенсуса (фактически децентрализованное администрирование и управление безопасностью).

Как представляется, приведенные выше подходы могут быть реализованы программным образом. При этом поддержка описанных функций должна быть реализована на уровне операционной системы, осуществляющей управление киберфизическим устройством.

Наделение киберфизических устройств функциями формирования безопасного «роя» может рассматриваться как одно из возможных направлений теоретических исследований и практических реализаций.

ВЫВОДЫ

Обеспечение информационной безопасности набора киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра», является актуальной научной и практической задачей. Решение данной задачи возможно путем наделения киберфизических устройств функциями формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности. Предложено реализовать указанные механизмы на уровне операционной системы, осуществляющей управление отдельным киберфизическим устройством.

СПИСОК ЛИТЕРАТУРЫ

1. Колосок И.Н., Коркина Е.С. Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. № 3 (15). С. 121-131. DOI: 10.25729/2413-0133-2019-3-11.
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М.: Книжный мир, 2009. 352 с.
3. Калинин М.О. Способ осуществления правил политики безопасности в одноранговых коммуникационных сетях киберфизических устройств. Российский патент 2020 года по МПК H04L12/721 G06F21/60. RU2714217C1
4. Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции: автореф. дис. … д-ра техн. наук. 05.13.19. Санкт-Петербург, 2019. 37 с.
5. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2 (30). С. 13–20.
6. Афанасьев М. Я., Федосов Ю. В., Крылова А. А., Шорохов С. А. Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов // Известия высших учебных заведений. Приборостроение. 2019. Т. 62, № 3. С. 226–234. DOI: 10.17586/0021-3454-2019-62-3-226-234.

Яви мне чудо

Егор Федоров
Республика Беларусь,
писатель, сценарист, драматург

"НЕЙК Эммануэль Мария – автор романа «Числа праведности», считающегося библией машинистов. В своих работах Нейк поднимает сложные вопросы жизни человека в современном обществе и выводит идеалы, к которым следует стремиться. Не рекомендуется к прочтению. Если вы обнаружите электронную или печатную копию романа «Числа праведности», немедленно сообщите об этом представителям власти. Спасибо за понимание".

"Детальный анализ «Чисел Праведности» показывает, что Эммануэль Мария Нейк хорошо изучила опыт становления существующих Традиций и создала книгу, способную заложить основы полноценного учения, весьма и весьма интересного современному человеку. Учения, ставшего порождением материального мира, а потому понятного каждому. Люди знают, что такое компьютер, сеть, программное обеспечение, легко увязывают все это в глобальное понятие «Цифра», оглядываются вокруг, видят, сколь глубоко проникла она в привычный мир, и задаются вопросом: «Где место Человека?» Нейк дает ответ: в слиянии. Нейк дает ответ: мы изменили мир и не должны бояться управлять им."

Вадим Панов. «Анклавы».

***

10:10

Дверь в нашу комнату распахнулась внезапно.

Настолько внезапно, что я сразу понял, что сейчас надо будет заложить руки за голову и опуститься на пол лицом вниз.

Что ж.

Рано или поздно это должно было случиться.

Однако, когда я оглянулся, я увидел, что торопиться ложиться на пол с поднятыми руками, видимо, не следует.

Нашу дверь уже захлопнула за собой и теперь закрывала на замок хрупкая девушка лет двадцати. Вместе с ней тёрся какой-то ботан в очках.

Девушка заперла дверь и обернулась к нам.

– Вы кто такие? – оторопел Заказчик. – А ну, пошли вон отсюда!!

Заказчик решительно поднялся.

– Пожалуйста, – проблеяла девушка. Она была бедственно, чудовищно перепугана. – Там какие-то люди. С автоматами. В коридоре. Прошу, вас. Они уже, кажется, кого-то убили…

– Что ты несешь? – Заказчик достал свой пистолет и снял его с предохранителя. – Отойди.

Девушка посторонилась.

Заказчик щелкнул замком двери, взялся за ручку, немного приоткрыл дверь и замер. По уверенности, с которой он действовал, было ясно, что это, скорее всего, бывший спецназовец. Или, там, десант – я особо не разбираюсь. Но я хорошо чувствую, когда человек понимает, что делает.

Заказчик, что делает, понимал.

«Заказчик».

Никакой он, собственно, и не Заказчик.

Даже Болт это понимал, хотя я с ним никогда не разговаривал на эту тему.

«True»-заказчики, настоящие заказчики – это совсем другой тип людей.

Видел я, конечно, и настоящих.

Но в основном мне приходилось иметь дело с такими вот «прокладками», которые мало понимали в том, что за информацию достаю я для них из сети.

Я уже давно научился отличать настоящего Заказчика от фальшивого.

Теперь подделка сделалась совсем уж очевидной – «True»-заказчик никогда бы не поперся с пистолетом в коридор, если бы узнал, что там находятся неизвестные вооруженные люди, которые уже, кажется, даже кого-то убили. Бесстрашие нашего теперешнего работодателя объяснялось ещё и тем, что он, как я подозреваю, что-то такое употреблял. Синтетическое. Но вполне допускаю мысль, что это была простая «отбитость» десантника. Или спецназовца.

Семеныч открыл дверь шире и выглянул в коридор. Видимо, никого там не увидел, вышел в коридор и пошел по направлению к соседнему офису.

В соседнем офисе работало человек пятьдесят. «Машинисты». Здоровенная такая комнатища с перегородками. И стеклянными стенами, отделяющими этот офис от коридора. Когда я шел к себе мимо этого офиса, я всегда задавался вопросом – зачем в нём стеклянные стены? Для того, чтобы машинисты стеснялись заниматься чем-то посторонним в рабочее время под взглядом прохожих? Как-то это было унизительно. Может быть, ещё и поэтому я никогда не помышлял о карьере честного айтишника.

Внезапно из коридора послышались выстрелы и меня даже подернуло от неожиданности. Болт сорвался с места, захлопнул нашу тяжелую дверь и стал закрывать её на замок.

– Рвать, рвать отсюда, – Болт обернулся с перекошенным от страха лицом. Он тяжело дышал. Кажется, у него началось что-то вроде панической атаки. Я никогда не любил Болта. Всегда он был какой-то суетный. И какой-то ненадежный.

– Заур, чего ты сидишь?! – завыл Болт. – Это же за нами, Заур!!!

Болт метался в беспорядке.

Интересно, что, по его мнению, я должен был делать?

– Заур! – причитал Болт. – Заур, нам доля, ты понимаешь? Ты понимаешь это, Заур?

– А если сейчас к нам постучат, ты уверен, что это будет не Семеныч? – я задал этот вопрос и даже немного удивился тому, как спокойно он прозвучал.

– Семеныча кончили, он в коридоре лежит, я видел! – Болт не смотрел на меня и я понял, что он врет. Внезапно Сережа остановился в своих метаниях, схватился за ручку фрамуги и стал распахивать окно.

Тут я подумал, что, может быть, Болт всё-таки видел труп Семеныча, там, в коридоре? Может быть, я зря так недоверчив к людям? Вдруг и впрямь сейчас постучат?

– Ты куда? – спросил я Болта.

– Лестница, – Болт смотрел за окно. Взгляд его светлел. – Вон же лестница! Заур, давай! Уходим!

Болт открыл вторую фрамугу и оглянулся на меня. Я посмотрел туда, куда указал Сергей. Лестница там действительно была. Однако была лестница совсем не рядом с нашим окном. До неё ещё надо было допрыгнуть. Я в сомнении посмотрел на коротенькие ножки и ручки Болта. Потом ещё раз на лестницу.

– Ну? – ещё раз спросил Болт меня, потом махнул на меня рукой и повернулся к лестнице.

Сразу Сережа прыгать не стал. Кажется, он понимал, что если недопрыгнуть, то дело обернётся если не совсем плохо, то нехорошо точно.

Тут из коридора снова послышались выстрелы. Кажется, Болтяра все же наврал. Семеныч всё ещё воевал там, за дверью. Впрочем, воевать могла и внутренняя охрана здания. Выглядели эти толстомясые, которые сидели на каждом этаже, не слишком боевито. Однако, не в туалетах же они сейчас отсиживаются? Я понимал, чего гадаю. Если в дверь постучат, то решать открывать или нет, придётся именно мне. Ладно. Будут бить – будем плакать. Постучат – тогда и решу.

Болтик оглянулся на входную дверь, за которой слышалась стрельба. Кажется, выстрелы его вдохновили. Он повернулся снова к лестнице, присел, оттолкнулся на своих коротеньких и пухлых ножках и выпрыгнул из проема.

И не допрыгнул.

То есть одной рукой лестницу он всё же схва-

тить успел, но рывок ста килограмм Болта мышцы этой руки уже не выдержали.

Болт заорал, когда понял, что лестницу он отпустил. Он неловко кувыркнулся вниз из-за инерции своего прыжка, ударился на прощанье о лестницу головой, отчего по всей по ней пошел глухой звук, и отправился в своё последнее путешествие. Лететь было не то, чтобы далеко – в здании было всего три этажа, и мы располагались на третьем. Но Болт ляснулся об асфальт так, что мне стало совершенно ясно – убился. Мысленно я снял шапку. Какой ни дрянной, а все ж человек.

Сергей был «факельщик». То есть он расставлял отвлекающие факелы, когда я взламывал сеть в другом месте. Функция Болта была в том, чтобы отвлекать на себя внимание Службы Безопасности той конторы, куда я пробирался.

Прощай, Болт.

Куда ты там попадешь после смерти, не ясно. Ясно одно – тебе уже не слиться с машиной.

Впрочем, когда мы разговаривали с Болтом об учении Нейки, он криво улыбался и всё подзуживал меня:

– Тебя тупо купили, – скалился Болтяра. – А знаешь, чем? Тем, что ты – айтишник. И тебе втулили новую религию, религию айтишников, понимаешь? Спешл фор ю, Заур.

Что ж. Отправляйся в тот мир, Болт, который тебе милее. Хотя и не помню я, Болтик, чтоб тебе был мил хоть один из загробных миров.

Выстрелы в коридоре стали реже, но не стихали.

– Кто-нибудь ещё желает попробовать? – я отвернулся от окна и посмотрел на тех двоих, с которых началась вся эта история. Они вразнобой, но однозначно отрицательно замотали головами.

Ручка нашей двери дернулась. К нам кто-то попытался войти.

Я не успел сообразить, что делать, если вдруг это всё-таки Семеныч. Без особенных пауз – видимо, пауза была только на то, чтобы отойти от двери – послышались выстрелы. Кажется, стреляли по замку. Не Семеныч. Уже хорошо. Выстрелили раз пять или шесть, пока не сообразили, что никакого урона эти выстрелы двери не причиняют. Дверь у нас была очень надежная. Врезалась сюда дверь с таким расчетом, чтобы у находящихся внутри было по крайней мере пять минут на уничтожение документации.

Эти пять минут сейчас надо было использовать на то, чтобы решить, что делать.

Решение возникло быстро. Может быть, потому, что оно было очевидным.

– Пошли, – бросил я на ходу, и направился к серверному шкафу.

Я открыл серверный шкаф, достал из него сервер, поставил на пол. В освободившемся пространстве открылся огромный календарь во всю стену с красивым вензелем «2028 год». Я открыл небольшую дверцу, что была скрыта за ним.

– Вперед, мои неожиданные друзья, – сказал я. – Навстречу приключениям.

Мой неожиданный друг любезно предоставил право пройти первой моей неожиданной подруге. Затем и сам полез следом за ней.

Когда неожиданный друг скрылся полностью, я закрыл за ним дверь. Затем я поднял с пола сервер, подошел к окну, поставил его сначала на подоконник, а потом выпихнул наружу. Сервер с грохотом упал на асфальт, совсем рядом с Болтом. Я выглянул. Ещё бы чуть-чуть и было бы неловко. И очень паливно. А так – вроде сойдет.

После этого я подошел к столу, сложил свой ноут. Затем вместе с ноутом я полез в серверный шкаф на место, которое освободилось от сервака и закрыл за собой дверь моего гробика. Места здесь не то, чтобы было много, но и скрючиваться или съеживаться почти не пришлось.

Тут я снова услышал шум в коридоре. Очевидно, что мальчики, которые захватили здание, вернулись и снова хотят сюда попасть. И обязательно попадут. А уже после того, как попадут, если мальчикам зачем-то понадобится открыть серверный шкаф, мальчики сделают мне больно.

– Ку-ку, – сказал я друзьям, которые находились сейчас в потаенной комнате за календарем «2028».

– Ку-ку, – глухо отозвался айтишник. – А ты чего не к нам? Здесь же хватает места.

– Чтобы вас, дураков, не нашли, – я мрачно улыбнулся своему ответу.

Не то, чтобы я был благородным парнем из

фильмов. Просто зачем? Если я тоже спрячусь в потаенной комнате, а мальчики после того, как войдут, начнут шмон, то потаенную комнату найдут на раз-два. А в том случае, если найдут меня, шмон на этом, скорее всего, закончится. И этих двоих искать уже никто и не будет.

– Всё, теперь ни звука, – сказал я. – Сейчас они будут ломать дверь.

– Я пон, – отозвался ботан.

Где-то в коридоре ухнул взрыв. Мальчики не придумали ничего другого, кроме как взорвать дверь. Оборудования они с собой никакого, очевидно, не прихватили. Только взрывотехническое. Ещё через минуту я услышал удары и затем послышался звук падающей на пол двери.

Затем стало очень тихо.

Я представил себе людей в балаклавах с автоматами, которые входят в комнату, страхуя друг друга. А может быть, с пистолетами? Да, пусть лучше с пистолетами.

– Никого! – услышал я юношеский голос. Правильно. Юноши должны идти впереди. Молодым везде у нас дорога, молодым везде у нас почет.

До меня донеслось шипение рации.

– Восьмой, восьмой, я Краб, – раздался из комнаты теперь уже другой голос. – В помещении никого нет. Окно открыто. Вижу под окном разбитую железную коробку и труп.

Голос немного подумал, потом решил поправиться:

– Скорее всего, труп.

Рация в задумчивости пошипела в ответ.

– Оборудование там есть? – спросила через треск рация.

– Ноутбук. Телефон.

Упс.

А про телефон-то я совсем и забыл. Осталось теперь молиться, чтобы про телефон не забыл Болт. Не забыл захватить его с собой в свой последний полет. Потому что если те, кто вошли, увидят два телефона, уж наверное они поищут второго обитателя этой комнаты.

– Один ноутбук и один телефон? – переспросила рация.

– Да.

– Забери оттуда всё и возвращайтесь. Отбой, Краб.

– Отбой.

Я услышал, как складывают ноут Болта, потом шаги, а ещё потом всё стихло. Я выждал несколько минут, потом толкнул дверь шкафа. Она открылась. В комнате не было никого. Я немного подумал, потом снова закрыл дверь.

– Сидим тихо десять минут, – сказал я своим друзьям. – Сейчас они могут вернуться.

– Я пон, – ответил ботан.

«Пон, пон».

Я думал, этот оборот уже давно вышел из обихода. Но смотри ты, молодежь тоже им пользуется. Я снова закрыл дверь своего гробика и устроился там как можно удобнее.

***

10:55

Меня зовут Заур Азгар.

Мне 41 год и я – «ломщик».

«Ломщик» – это тот, кто проникает в чужую систему для того, чтобы добыть информацию. В этом офисе на улице Панерю города Каунаса я оказался позавчера. А ещё два дня назад я был в городе Кыюве на улице Крещатик, где у меня двухкомнатная квартира прямо под небом, на двадцать восьмом этаже.

Не то, чтобы я был очень уж крутым «ломщиком». Но в топ-50 «ломщиков» мира я, кажется, вхожу. Входил по крайней мере ещё в прошлом году. В этом году я даже ещё и не поинтересовался своим местом в этом списке. Уже не так интересно. Уже не так горят глаза. Это для молодых всё – рейтинги, прыжки и вертикальный взлет с помощью пламени из пятой точки, которое вырывалось и у меня лет до тридцати пяти. Теперь пламени уже почти нет. Заказы есть – хорошо. На хлебушек заработал – и ладно. Хлеб я, правда, давно привык есть белый. И чего-то люблю, чтоб с икрой.

На этот заказ в Литву мне ехать не хотелось.

Я знал, что государственная власть здесь провисла сильно. Сильнее даже, чем на Украине. Из этого вытекало то, что если меня отследят, то получится совсем не очень. Анклав «Basf», в чью систему мне предстояло залезть, не будет стесняться того, чтобы нас «накрыть».

Примерно так и произошло.

Что делать теперь, представлял я слабо. Ни-

каких планов на отход у «ломщика» почти никогда нет. Хотя бы потому, что работать приходится всё время из нового места.

Но часов десять на размышления сейчас, кажется, было. Я оставил свой информационный след сразу в трёх больших офисах здания. Таких же офисах, как тот, что по соседству, то есть человек на 50. Так что мальчикам из «Basf» ещё очень долго придётся разбираться с тем, что содержат машины этих офисов, прежде чем они поймут, что следы ведут именно сюда, в эту комнату. А пока… Пока сюда никто не должен был прийти вообще. Но минут десять нужно было сейчас выждать. Мальчики могут захотеть вернуться с дополнительным осмотром помещения. Я засек время на своих наручных часах.

Где-то в коридорах и других помещениях здания шла жизнь, где-то она даже кипела. И я слышал отзвуки этого бурления. Но достаточно глухо. В нашу комнату никто не заходил. Я посмотрел на часы. Десять минут прошло. Я снова открыл дверь своего шкафа и выбрался наружу. Огляделся.

Дверь в наш офис сейчас в проеме отсутствовала – она в каком-то бессилии лежала на полу. Я ещё раз подумал над тем, что именно нам может пригодиться в нашем убежище. Взял с пола литровку, в которой осталась ещё кола, которую пил Болт, вылил остатки в мусорку и налил в бутылку воды из кулера. Открыл шкафчик, взял пакет из Мака. Это был мой завтрак. Зарядное от ноута. Кажется, всё? Я пошел к серверному шкафу. Забрался в него, закрыл за собой дверь потом открыл дверь потаенной закабайки и забрался внутрь.

Ботан сидел на ящике. Когда он увидел меня, он отложил телефон, который держал в руках. Девушка сидела в углу.

– Можно? – спросил я.

– Хлеб-соль, – ответил ботан.

Вроде не зануда. Это хорошо.

Скорее всего, раньше это была какая-то кладовая. Такие тайные помещения, по моим прикидкам, есть в каждом третьем большом офисном здании. Всерьёз обмануть кого-то этим невозможно, то есть при тотальном шмоне этот тайник быстро найдут. Но на тотальный шмон ещё надо напороться. А просто хранить какое-то оборудование, которое не предназначено для чужих глаз, такие помещения подходили вполне. Примерно половину нашей кладовки и занимало это оборудование. На второй половине места оставалось достаточно.

– Заур, – представился я. – Предприниматель.

– Дима, – отозвался ботан. – Криптограф.

– Екатерина, – сказала девушка и торопливо поправилась, – Катя. Художник компьютерной графики. 2D.

Сейчас я разглядел Катю лучше.

Катя показалась мне очень даже ничего. Хоть и была она сейчас сильно напугана.

– Скажите, – попросил ботан. – А что происходит?

– Давай на «ты», – предложил я. Очкарик кивнул.

– А что в этой твоей машинке пишут? – я показал пальцем на его телефон.

– Что здание захватили неизвестные. Требования их не ясны.

– Ну? – спросил я. – И чего же ты хочешь от меня?

Я достал из-за пазухи свой ноут и поставил на один из ящиков.

– Ну, вы… То есть «ты». У меня сложилось впечатление, что ты что-то понимаешь в происходящем.

– Почему?

– Ну этот, который выпал из окна, – очкарик, очевидно, раздумывал обо всем этом пока дожидался меня. – Он говорил что-то такое…

– Какое? – какой, однако, деликатный ботан.

– Ну… Как будто это за вами пришли.

– А.

Болтик, Болт. Сереженька , Сергей. Сейчас выпутывайся из того, что ты на прощание наговорил.

– У него была истерика, – сказал я. – Мы здесь занимались не совсем законными делами. Но не того масштаба, чтобы снаряжать против нас армию.

– Заяц думал, что танковая атака направлена против него, – неожиданно сказала Катя и слабо улыбнулась.

– Именно так, – я улыбнулся Кате. Какая интересная, наверное, девочка.

Я открыл свой компьютер и стал закрывать ставшие уже ненужными окна.

– А что видели вы? – спросил я, не отрываясь от работы. – Ну там, в коридоре?

Очкарик пожал плечами.

– Да собственно, что.... – сказал он. – Мы возвращались с обеда. Со второго этажа. Шли к себе... Вдруг видим, что в нашем офисе какие-то люди с автоматами. Кого-то избивают. Кого-то кладут на пол. Испугались. Прошли мимо нашего офиса. Следующее помещение – ваше.

– Кого-то действительно убили? – я посмотрел на Катю.

– Нет, – ответила Катя. – Ну, то есть я не видела, чтобы кого-то убили.

– Зачем же вы врали? – спросил я.

– Я очень испугалась. Я боялась, что вы нас прогоните, – ответила девушка. – Но били они... ну эти, с автоматами, очень крепко. Я видела Борю, нашего менеджера, у него всё лицо в было в крови.

– Ясно, – сказал я. – Ну что ж. Давайте ждать. Мне кажется, рано или поздно они уйдут.

На самом деле, мне так, конечно, не казалось.

Пока люди из «Basf» не нашли того, за чем пришли, они никуда не уйдут. И никакая полиция их отсюда не выкурит. Даже и пытаться, я думаю, особенно не будет. Потому что «Basf» – это Анклав. А Анклавы сейчас сильнее почти любого правительства. Литовского правительства – сильнее точно.

– Да, будем на это надеяться, – улыбнулся ботан. Тут он что-то вспомнил. – Ой, Заур, я тут... В общем, у вас тут коньяк стоит, я глотнул немного. Вы уж извините.

– Коньяк? Ну это не у меня, – я закончил со своим ноутбуком и открыл новостной портал. – Коньяк, говоришь...

Болтяра. Я точно знал, что он закладывает. Видимо, прятал здесь большую какую-то тару, отливал из неё во флягу. Я однажды видел эту его фляжечку, небольшая, грамм на двести. Спрашивать не стал, что в ней. И так было ясно. Мы здесь оставались порой и на ночь. Попробуй, протяни целую ночь без выпивки. Наведывался Болт сюда по прямым своим обязанностям – принести-подать. Какое-то оборудование мы использовали час-два, потом его необходимо было занести обратно. Когда Болт сюда наведывался, он и наполнял свою фляжку.

– И что, хороший коньяк? – спросил я.

Ботан поднялся полез за ящики и достал здоровенную красивую бутылку.

– Заур, может быть вы тоже выпьете? – спросил меня очкарик.

– Нет, я не пью, – ответил я на автомате.

Потом я посмотрел на этикетку. А неплохо Болт зарабатывал, явно дорогой коньяк.

Я смотрел на почти целую красивую бутылку коньяка ёмкостью в один литр и меня все больше охватывали сомнения.

А какого, собственно, черта я не пью?

Чтобы подольше пожить? Без болезней там? Без черноты от похмелья? Без крови из носу, без чего-то сверлящего в правом боку?

Так ситуация пока выглядит так, что через десять часов мои планы на дальнейшую жизнь не будут иметь никакого значения. Если меня возьмут, то сначала достанут из меня всю информацию, которая им нужна. А потом вальнут. Вальнут-вальнут. Это совершенно точно.

Так какого же это черта тогда я не пью?

На минуту встал передо мной приемный покой наркологической клиники «Парацельс», где я отходил в последний раз от «заплыва». Унизительный допрос у врача, игла капельницы, санитарка с ведром, таблетки, таблетки, снова капельница.

После того случая я завязал и не пил вот уже почти год. Иногда рюмку или две, не больше. Потому что если больше – фокус происходящего вокруг для меня смещался. И я уже просто не понимал, отчего это мне не выпить ещё. Алкогольная реальность была много милее и симпатичнее этой. Головой я прекрасно понимал, что это был морок, наваждение. За которое потом приходилось расплачиваться в том же «Парацельсе».

Но сейчас до «Парацельса» мне было, как до Луны. А может быть, и ещё дальше.

Очкарик после моего ответа вздохнул и полез ставить бутыль туда, откуда её взял. Кажется, он не отказался бы выпить ещё и был разочарован моим ЗОЖем.

– Впрочем, погоди, – остановил его я. – Давай. По стаканчику.

Ботан улыбнулся и я словил себя на мысли, что никакая он не молодежь – очкарику было

тоже, кажется, уже лет под сорок. Просто сохранился лучше, чем я. Тут я понял, что он представлялся, но я совсем забыл, как его зовут. Со мной такое случалось. Ненужная информация просто не проходила фильтр и не сохранялась. Катю вот как зовут я запомнил, а ботана – нет. Но это ничего страшного. Сейчас познакомимся ещё раз.

Меня охватило радостное возбуждение, знакомое всем алкоголикам, которые собирались вот-вот «развязаться». Причем было почти неважно, «развязаться» после трёх сухих дней или после года воздержания.

– Стаканов только нет, – Ботан протянул мне бутыль – Ну и запить там, или заесть тоже.

Очкарик как будто оправдывался за столь плохую встречу гостей.

– Есть, и запить у нас теперь есть, и закусить, – сказал я.

Я залез в пакет и достал бутылку с водой. Следом я достал пакет из Мака, положил на стол и развернул.

– Ой, а можно тогда и я выпью, – подала Катя голос. – Если запить есть. Я без воды не могу.

– Конечно, – ответил я. – Прошу.

Катя поднялась, подошла, приняла у меня бутыль, неловко сделала небольшой глоток, сморщилась, запила и отдала бутыль мне.

Я выдохнул и сделал глоток куда как более мощный, чем Катя.

Тут же почувствовал, как внутри коньяк разлился и согрел меня где-то там, в животе.

«Поплыву сейчас», – пронеслось в голове.

Я отщипнул себе от бутерброда и передал бутылку с коньяком ботану.

– Давай, – сказал я. – К столу.

***

13:31.

– Повторяю, здание окружено. Предлагаем вам отпустить остальных заложников и начать переговоры о сдаче.

Голос из громкоговорителя был немного похож на голос Юрия Левитана, который объявлял о начале Великой Отечественной войны. Такой же он был торжественный и печальный.

Мы устроились в нашей комнате как-то даже и уютно. Оборудование здесь было укрыто покрывалами – видимо хозяин этой точки «ломщиков» отличался большой бережливостью. Катя куталась сейчас в одно из этих покрывал – видимо, девочка замерзла у стены. Мы с ботаном устроились полулежа вокруг нашего стола. Закуску уже доели, воду почти допили.

– Остальных? – спросила Катя, после того, как громкоговоритель умолк. – Значит, часть заложников они отпустили?

– Ну конечно , – ответил я. – Здесь человек 500, наверное, работает. Какие-то офисы совсем не связаны с областью ай-ти.

– Ну мало ли, кто чем может заниматься в своём офисе, – сказал Дима.

– От «балалайки» род занятий не укроешь, – лениво парировал я. – Слишком палевно. Если вшито, что ты менеджер по продажам, то, как правило, так оно и есть. Ну и у «Basf», наверняка есть оборудование, чтобы проверить, лазили в «балалайку» или нет.

– А, – сказал очкарик. – Вообще да.

– Повторяю, – снова завел свою шарманку голос из громкоговорителя. И стал повторять весь тот текст, который мы уже слышали.

– А как они отсюда уйдут? – сказала Катя. – Не будут же они воевать с полицией?

– С полицией они воевать не будут, – ответил я.

– Что тогда? – спросил Дима.

– Прямо над нами – вертолётная площадка.

– И что же, – не понял ботан. – Им вот так вот запросто дадут уйти?

– Дадут, – сказал я. Меня клонило в сон. Этой ночью мы с Болтом почти не спали. Коньяк же приятно размазывал меня по полу. Я закинул руку, согнутую в локте, на лицо, облокотился на какую-то коробку и занял как можно более горизонтальное положение.

Никакого плана спасения за прошедших два часа у меня так и не родилось. Положа руку на сердце, я его совсем и не обдумывал. Чего-то не хотелось. Хотелось «бухать и кружиться», как говорил один мой приятель. Хотелось болтать о чем-то совсем неважном.

– У тебя есть погоняло, Дима? – спросил я.

– Нет.

– А когда-нибудь было?

– Ну, в школе пытались чего-то. Ни одно не

прижилось.

– Скучный ты человек, – сказал я. – А у «ломщиков» не бывает так, чтоб без «погоняла». Без рабочего имени.

– Так вы «ломщик», – не вопросительно, а скорее утвердительно сказал ботан.

Я прикусил язык. Алкоголь. А впрочем, подумал я с какой-то пьяной бесшабашностью, сейчас не все ли равно?

– «Ломщик», да, – ответил я.

По паузе, которая возникла, было понятно, что у ботана вертится ещё какой-то вопрос, но задавать его он не стал.

– Ну что, попробует кто-нибудь угадать моё рабочее имя? – снова спросил я.

– Скажите тоже, – отозвалась Катя. – Тут же бесконечно можно гадать.

– Да, – согласился я. – Тогда даю вам подсказку. Моё рабочее имя получилось из моего настоящего имени. А зовут меня, напомню, Заур.

– Зорро? – спросил ботан. – Ещё могу предложить «Ур».

– Заза, – сказала Катя.

– Мимо всё, – ответил я. – Ещё будут предложения?

Предложений больше не было.

– Изаура, – торжественно сказал я.

Никто не засмеялся.

– Что, не смешно? – спросил я.

Мне не ответили.

– Я когда имя «Изаура» в юности увидел – обомлел, – пустился я в объяснения. – Представил на секундочку, что кто-то, кроме меня ещё увидит это вот «И-заур-а». И попробует меня так называть. Это же драться придется, думал. А если и драться не поможет? А если и не отлипнет вовсе, думал. Что тогда?

Я тихонько засмеялся.

– Несколько ночей не спал, помнится. Но ничего. Обошлось А вот когда я уже вырос и стал «ломщиком» сам себе это имя и выбрал. В качестве рабочего.

– Такая победа над детскими страхами? – спросила Катя.

– Да, – сказал я. – Что-то вроде того. А ещё очень удобно в том плане, что маскирует. Сейчас, вполне возможно, «Basf» ищет девушку-ломщика.

Я поднялся на локте, протянул руку к бутыли с коньяком, сделал глоток, запил, и предложил ботану.

– Э? – сказал я.

– Э, – согласился очкарик. Он взял бутыль и тоже выпил.

Последний глоток настроил меня на философский лад. Я принял прежнюю позу, закинул для удобства ногу за ногу и спросил:

– А что, Дима, – решил я затронуть вопрос, который меня сейчас действительно волновал. – Боишься ли ты смерти?

Я заподозрил в ботане лютого атеиста и мне стало интересно с ним покалякать о Нейки. Редко когда я разговаривал о Традиции с кем-то посторонним. Почему бы не сделать это сейчас?

Ботан некоторое время молчал, потом сказал совсем не то, о чем я его спрашивал:

– Так всё-таки всё, что происходит – из-за вас? – Он подумал и добавил. – И что же, если вас найдут, вас обязательно грохнут?

– Оставим в стороне этот ненужный сейчас вопрос, Дима, – ответил я. – Давай лучше поговорим о смерти в целом. Давай лучше поговорим о том, что будет после того, как ты умрешь. Ну, или я. Неважно. Ну?

– Да что будет, – после недолгого молчания сказал ботан. – Ничего. Гроб, кладбище черви и черная пустота.

– И всё?

– Ну да, – ответил мой собеседник.

Я внутренне покивал сам себе головой. Ага, ага, упоротый атеист. Ну что ж. Быть может, получится интересно.

– А тебе не кажется, Дима, – сказал я и закинул руку за голову. – Что если впереди только гроб, кладбище, черви и черная пустота, то ты сейчас находишься в такой… ммм… подлодке, которая не то, чтобы уже затонула. Но которая уже совершенно точно никогда не поднимется на поверхность?

– Не очень понимаю эту сентенцию, – сказал ботан.

– По-моему, очень просто, – я сделал ещё глоток из бутылки. – В этой подлодке ты плывешь, конечно же, не один. Много вас таких. У кого кроме червей и пустоты в перспективе ничего не рисуется. Плывете, стало быть. Воздуха

в вашей подлодке достаточно и хватит ещё надолго. Еды в подлодке припасено тоже с избытком. Есть библиотеки, спортзалы, кинотеатры. Друзья и коллеги с тобой, как я уже говорил, плывут – вы этой подлодкой вместе все управляете. За окнами иллюминаторов вашей субмарины бывает красочно, красиво и захватывающе. И даже в одном из отсеков, давай сделаем такое допущение, девки присутствуют.

– То есть всё в вашей подлодке вроде как и есть, – продолжил я. – А вроде как и совершенно ясно, что воздух когда-то в вашей субмарине закончится. И когда это произойдет, всем вам в этой подлодке наступит конец. И вам, и друзьям вашим, и девкам, которых вы, вполне возможно, успели уже даже полюбить.

– А что вы скажете за моих детей? – спросил очкарик. – У меня их двое. И они тоже не верят ни в какую загробную жизнь.

– За твоих детей я тебе, Дима, скажу, – ответил я. – Что время от времени к вашей подлодке швартуется другой, точно такой же подводный корабль. С ограниченным запасом кислорода. И ваши дети пересаживаются в него, когда приходит время. Затем они отчаливают. В своё собственное, индивидуальное, но совершенно, согласись, идиотское путешествие. Которое ничего не предполагает кроме того, что когда-то и в их субмарине закончится кислород.

– Гм..., – Дима помолчал. – Хорошо. Но что же мешает мне подняться к поверхности, чтобы пополнить запас кислорода?

– Ты, Дима. – я ткнул пальцем в собеседника. – Ты сам и мешаешь.

– Отчего же? Я непроходимо дремуч? И не понимаю, что этот запас можно пополнить?

Я искренне рассмеялся.

– Я об этом даже как-то не подумал. Но всё верно, – ответил я. – Ты и все вы в этой подлодке непроходимо дремучи. Но только в этом вопросе. Вы прекрасно разбираетесь в румбовых системах и угловых скоростях, в акустических размыкателях и пеленгаторах, а лучше всего вы разбираетесь в знаках различия на форме. Но вы не подозреваете элементарного. Вы не подозреваете, что поверхность существует. И что туда можно всплыть.

Помолчали.

– И за какую религию вы топите? – спросил ботан.

– Ни за какую, – ответил я. – Если говорить о том, что мне интересно по данному вопросу, то интересно мне учение Нейки. Что-то слышал об этом?

– Новые сектанты, – сказал ботан. – Нет, не слышал. Давненько уже не слежу за всем этим. Не вижу смысла.

Я почувствовал, что он меня задел. Сектанты. Надо же.

– Нейкизм – это не секта и не новая религия, – сказал я. – Нейкизм – это Традиция.

– Суть, мне кажется, от этого не меняется, – сказал очкарик. – Кстати, отчего вдруг «традиция»? Насколько мне известно, «традиция» – это что-то, что создавалось веками. А ваш этот нейкизм... Ну сколько ему?

– По-моему понятно, что у любой Традиции должно быть начало.

– А, – ответил очкарик скептически. – Вот в чем все дело. И что этот Нейки? Это ваш новый Христос?

– Нейки – это женщина, – ответил я. Эммануэль Нейки. Она написала книгу «Числа Праведности».

– Ну, допустим, – пожал плечами ботан. – И какое же в этой вашей традиции обещание?

– Не понял?

– Что здесь непонятно, – ботан встал, чтобы размять ноги. – Любое такого рода учение должно что-то обещать. Потому что появляется весь такого рода шлак из-за страха, неужели вам это не ясно? Ведь вы, кажется, умный человек. Из-за страха смерти появляется, понимаете? Больше не из-за чего. Ну неохота человеку умирать, мозгу его в первую очередь никак не хочется признавать такой факт – что он умрёт. Что все то, что когда то родилось, всё, что стало живым, обязательно станет и мертвым. Обязательно. Всё без исключений. А мозг – штука очень хитро устроенная. В особенности, если это мозг человека. Уж сколько там воображения, сколько фантазии! А тут – такая шикарная точка приложения. Как бы это мне так сделать, чтобы не умирать, думает ваш мозг. И фантазирует, такой. И воображает.

Ботан подошел, взял бутылку и сделал из неё глоток. Кажется, он дразнил меня. Ну что ж.

– В средние века человек умирал от баналь-

ного аппендицита. В страшных мучениях. Потом ему это надоело, он нашел причину и научился бороться с этим. Всё это он сделал при помощи своего мозга. Это, по-твоему, тоже проявление фантазии, проявление воображения?

– Нет, – ответил ботан. – Это – нет.

– А отчего ты решил, что разобраться с проблемой смерти – это из какого-то другого ряда?

– Да потому что всё живое – конечно! Потому что тут нет пути. Тупик, понимаете?

Ботан поставил бутыль и пошел на свое место.

– Мне чего-то мерещится, что тем, кто хотел перемещаться не по земле, а по воздуху, говорили примерно то же самое, – сказал я.

– Да не то же самое! – сказал Дима. – Если уж переходить в техническую плоскость, то вы, по сути, хотите создать вечный двигатель. Который , как известно, невозможен!

– Кекеке, – сказал я. Подумал, может быть действительно поговорить с очкариком в технической плоскости? Но решил, что нет. Точно не сейчас. – Ты не прав.

– Почему?

– Хотя бы потому, что пока никто не знает даже близко, что такое жизнь и как превратить мертвое в живое. В отличие от упомянутой тобой технической плоскости, где человечество продвинулось значительно в поисках Знания. Здесь же, в вопросах жизни и смерти, люди пока ещё находятся в самом начале пути.

– Ну прям, – сказал ботан. – Техника стала развиваться худо-бедно пятьсот лет назад, а буддизму, к примеру, две тысячи пятьсот лет. По иудейскому календарю и вовсе сейчас шестое тысячелетие.

– Техника начала развиваться с изобретения колеса. А это было чуть ли не семь тысяч лет тому назад.

Я задумался о том, что сказать дальше. Тут новый глоток коньяка добрался до моего нутра и я снова окрылился.

– Хорошо, Дима! – сказал я. – Может быть, ты прав! Может быть, все колеса в этом вопросе уже изобретены. Но! Но, Дима, но! Кроме того, что колеса уже изобретены, эти колеса уже успели сильно износиться! Если пользоваться этой аналогией, то телега уже не едет на этих колесах! Застряла! Потому что колеса эти выщербленные, горбатые и кривые от времени.

– И что?

– А то, что миру нужны новые колеса, Дима! – сказал я. – Скажи мне, Дима. Что может быть новым …ммм… учением о вопросах жизни и смерти сейчас, в нашем благословленном 21-м веке?

– Ну, – пожал плечами ботан. – Вероятно, это должно быть что-то, связанное с цифрой.

– Верно, – я поднялся и ткнул пальцем в оппонента. – И будет! Это учение обязательно будет связано с цифрой!

Тут я заметил Катю, которая пялилась, в свою очередь, на меня. Должно быть, выглядел я горячим парнем. Может быть, она подумала, что я сейчас кинусь и задушу своего собеседника.

– Понимаешь, будет! – сказал я. – Обязательно будет, что-то связанное с Цифрой! Эра новая настала, Эра Цифры. И этой эре обязательно нужна новая Традиция, не может быть по-другому. А то, что сейчас мы, «ломщики» пытаемся эту традицию зародить – так это нам большой респект и уважуха, Дима! Чем быстрее мы перенесем телегу на новые колеса, тем быстрее мы отправим эту телегу снова в путь. И состоится новый виток развития.

Я подхватил пластиковую литровку, встал и пошел на выход из нашего убежища.

– Я за водой, – бросил я своим неожиданными друзьям.

Я выбрался из нашего убежища, замер, постоял и послушал. Сейчас было тихо.

Я набрал воды из кулера. Пока она наливалась, я подошел к окну ещё раз и оценил расстояние до пожарной лестницы. Нет, до неё я не допрыгну точно. Болтику было лет двадцать пять. Мне сорок. Физическими упражнениями я себя не утруждал, прыжками в длину не увлекался. Без шансов, однозначно. Я оглянулся в поисках чего-нибудь, что помогло бы мне попасть на лестницу. Решительно ничего, кажется, нельзя было приспособить с этой целью. Я стоял посреди комнаты, смотрел на лестницу и с тоской думал о том, что спасти меня теперь могло только чудо.

«Господи, яви мне чудо...» – вспоминался мне шестнадцатый Псалом.

Я выключил воду, забрал бутылку и вернулся к своим друзьям.

– Спасибо, – сказал ботан, когда я протянул ему воду.

– Мне кажется, что если вы и перекладываете телегу на новые, годные колёса, – сказал ботан и отдал мне воду. – То направление, по которому вы хотите эту вашу телегу перемещать, никуда не ведет, кроме как в дебри дремучести и невежества.

– Какой ты, однако, упоротый, – сказал я. – По-твоему, мы хотим вести людей не к с свету, а во тьму?

У меня начало уже подгорать и дымиться.

– Что вы хотите не важно, – умничал дальше очкарик. – Вы же прекрасно знаете… Благими намерениями…

– Ведет дорога в ад. Которого нет, – сказал я.

– Конечно, нет, – сказал очкарик. – Ни ада нет, ни рая, ни бога, ни черта. Ни домовых, ни шишимор, ни призраков, ни неприкаянных душ. Все это придумали люди, ну неужели вам это не ясно? Люди! Скучно им было. Вот и придумали!

– А вы знаете, Дима в чем-то прав, – сказала художница из своего угла. – Я сама неоднократно задумывалась об этом.

– О чем именно? – спросил я.

– Мне ведь приходится рисовать новых сущностей для компьютерных игр, – сказала девушка. – То есть я придумываю то, чего раньше никогда не было. И не раз у меня мелькала такая мысль. Если я способна придумать и придумала уже с десяток новых персов, то что мешало людям древности придумать всех этих подселенцев и леших, оборотней и суккубов, лярв и волколаков?

– Вот. – поддержал Катю ботан. – Тем более, что таких фантазеров и не надо было много. Горсть всего нужна. Люди прошлого не были избалованны компьютерными играми или фильмами ужасов. И если кто-то придумывал вервольфа, его тут же подхватывали и несли с радостью в массы.

– Что-то я не очень понимаю, при чем здесь вервольфы и волколаки, – сказал я.

– Да при том! – ответил очкарик. – При том, что все религии – это тоже чья-то фантазия, выдумка. Плод работы чьего-то мозга – мозга, бегущего от страха смерти – и ничего больше! Только с этого ещё можно иметь очень хороший профит. Сделать из этого бизнес. По-моему здесь всё настолько прозрачно ясно, что и обсуждать нечего!

Он помолчал.

– Доказательств нет, понимаете? – сказал очкарик. – Вы хоть раз были свидетелем чуда, Заур?

Меня уже всерьёз стал раздражать этот разговор. Но что ответить, я не нашелся.

– Нет, не были, – уверенно сказал очкарик. – Вам лет, наверное, сорок, а вы за все эти сорок лет не видели ни одного чуда. Ничего не заподозрили до сих пор? Может быть, чудес не бывает?

Я почувствовал, как внутри у меня что-то замкнуло. Десять минут назад я стоял у окна в комнате и думал о чуде. Сейчас этот ботан говорил о том же. А ведь действительно, сейчас, кажется, самое время для чудес.

– Хорошо, – сказал я. – Будет вам сейчас чудо.

– Что же, прямо сейчас? – осклабился ботан.

– Ну, не прямо сейчас, – ответил я и почувствовал себя неловко. – Некоторое время мне всё же понадобится.

Я потянулся за своим ноутом.

Дело в том, что…

***

Дело в том, что Эммануэль Нейки в своих «Числах праведности» давала некий набросок, некую тропу, которая позволяла бы добраться до самой вершины, до конечной точки в Традиции Нейки.

Точно также в своих трудах (правда изустных) это делали Будда или Христос.

В Христианстве такой точкой являются Преображение и Спасение, которое есть избавление человека от греха и его последствий — смерти и ада, и обретение спасённым человеком Царства Небесного. Преображение же – некая трансформация, в результате которой человек станет уже кем-то другим.

В Буддизме всё тоже самое. Только слова иные – Прибежище и Выход из Сансары. Аналог христианского «спасения» – «прибежище» – можно сравнить с пещерой, куда прятался древний человек от непогоды и диких зверей.

Такими пещерами сейчас для большинства людей являются деньги, алкоголь, наркотики, лекарства, некоторые ищут прибежища даже в сексе. Рано или поздно к почти каждому приходит понимание, что все эти перечисленные пещеры – фальшивые. Что всё это – декорации пещер.

Когда наступает это понимание, иногда бывает ещё не поздно поискать настоящую пещеру, настоящее «прибежище». Со мной, кажется, был именно тот случай.

Когда я читал «Числа Праведности», я сообразил, что Слияние с машиной, о котором в «Числах» очень много говорит Нейки, подобно христианскому преображению или буддистскому выходу из круга сансары.

Но что будет в Традиции Нейки Спасением (или Прибежищем), я понять не мог. По всей видимости, это был машинный код. Но никакой уверенности у меня в этом не было.

Тем не менее, я стал набрасывать черновой код для Слияния, который, как казалось не только мне, был прописан в «Числах Праведности». Этот код, конечно же, нельзя было прописать единым для всех – он строго индивидуален и основан на особенностях того, кто пишет этот код. Понимаю, что и тут прослеживается аналогия с тем, что Будда никогда не давал двух одинаковых наставлений разным людям, а Христос мог говорить разные проповеди – иногда диаметрально противоположные. Но что делать, Традиция есть Традиция. Инструментарий у человека такой. Не самого широкого спектра. И потому все Традиции всегда будут похожи друг на друга. Я рискну предположить даже большее – если в какой-то Традиции будут отсутствовать некоторые обязательные компоненты, то такую Традицию надо вычеркивать. Это все равно что попытаться сделать плов без, скажем, риса. Или мяса. Или не добавлять воды. Не хватает одного из компонентов – не будет плова. Может, конечно, и получится что-то съедобное, но пловом это не будет.

В общем, читал я и перечитывал «Числа Праведности», постоянно находил там для себя что-то новое, писал и переписывал свой код, изменял, добавлял и перекраивал. Но никогда я этот свой код не запускал. Знаете, почему? Потому что мне нравился этот мир, в котором я сейчас нахожусь. Меня устраивал мой образ жизни, моё здоровье, моя семья, моя работа и состояние моих денежных активов. Меня устраивало почти всё. Куда и зачем мне преображаться или выходить из сансары? Незачем, совершенно. Куда мне было спешить? Наверняка должен был бы наступить такой день, когда меня перестало бы устраивать многое в этом мире. И к этому дню я худо-бедно был готов.

Ещё я не запускал мой код, потому что не имел безоглядной веры в то, что из этого что-то должно обязательно получиться. И получиться должно было именно то, чего хотелось, а не что-то другое. Даже тогда, когда стоишь в дверном проеме самолёта с парашютом за спиной, у тебя нет никакой уверенности, что с прыжком получится так, как задумывал, впереди – совершенная неопределенность. Ну и если сравнивать с прыжком с парашютом дальше, то сейчас мой парашют укладывали не специальные люди, которые уже уложили до этого сотни парашютов, а я сам. Да что там укладывал – я даже сшил этот парашют сам. Эммануэль Нейки, в сущности, мне только дала материал, из которого я мог шить свой парашют.

И вот сейчас, кажется, наступил тот момент, когда мне его нужно использовать.

По моим прикидкам, у меня ещё было где-то четыре часа.

За это время предстояло превратить черновик кода в его чистовик.

Как-то неожиданно скоро мне понадобилось это сделать. Внезапно. Вдруг.

«Я думал, у нас в запасе ещё как минимум лет пять».

Я положил свой ноут на колени, раскрыл его и открыл папку «Нейки».

***

0:10

Они сидели за столиком в кафе на улице Панерю, куда почти каждый день ходили обедать. Уже наступила ночь.

Перед Катей стоял дымящийся кофе, Дима заказал себе литр грейпфрутового сока и почти половину графина он уже опустошил. Пить Дима хотел чудовищно. Первым делом, когда их отпустили, Дима зашел в офисный туалет,

набрал в рот водопроводной воды, но глотать не рискнул – просто прополоскал и сплюнул. И только уже здесь, в кафе, отвел душу.

– После всего, что между нами было, – сказал Дима и поставил стакан на стол, – я, как честный человек, должен теперь на тебе жениться.

Кате шутка понравилась. Она улыбнулась.

– Да уж, – сказала она. – На всю жизнь приключение. Ты спать не хочешь?

– На удивление нет, – ответил Дима и улыбнулся. – Наверное, ещё адреналин в крови гуляет.

Дима посмотрел в сомнении на свой графин. Сока больше не хотелось.

– А ты здорово держался, когда они к нам вломились, – сказала Катя. – Я, честно говоря, на несколько секунд сознание потеряла от страха.

Дима обернулся к бару и поднял руку.

– Сто пятьдесят коньяку, – сказал он, когда подошел официант.

– Какого?

– Гм, – Дима вдруг вспомнил события прошлого дня. Коньяка захотелось сейчас именно такого, какой они пили там, в подполье. – А у вас есть этот, как его… Что-то «стр…»

– «Mistral»? – спросил официант.

– Вот, да, – щелкнул пальцами Дима. – Его, пожалуйста.

– Эйн момент, – сказал официант и удалился.

– Я, честно говоря, тоже кирпичей отложил будь здоров, – сказал Дима. – Просто старался, как мог… Лицо сохранить, что ли. В конце концов, перед тобой было бы потом очень неудобно.

Официант принес коньяк и два бокала. Дима понял, что о Кате он и не думал вовсе, когда делал заказ и мысленно поблагодарил официанта. Официант разлил коньяк по бокалам и удалился.

– Ну что, – сказал Дима. – За то, что хорошо заканчивается?

– Да, – Катя тоже подняла бокал.

Они выпили.

– Заура этого, конечно, очень жаль, – сказала Катя. – Как ты думаешь, что с ним произошло?

– Да, – ответил Дмитрий. – Жаль. Несмотря на всю эту дурость про загробные миры, наверняка хороший был человек. А что с ним произошло… Ну откуда же мне это знать. Может быть, дело в алкоголе. Помнишь, он говорил, что непьющий? Может быть, зашитый был или что-то в этом роде. Выпил… Ну и, в общем… Двинул коней. Выпил то он очень прилично.

– Но какое-то странное совпадение, – сказала Катя. – Он же печатал что-то там у себя в ноуте, даже когда они уже ломились.

– Ну тогда, может быть, сердце, – сказал Дима. – Он ведь знал, что его ждёт, когда его возьмут. Не зря же этот, как его…второй этот.

– Болт.

– Ага. Не зря же этот Болт в окно кинулся.

Некоторое время помолчали.

– Я думала, сейчас пойдем по этому делу, как сообщники, – сказала Катя.

– Могли, – отозвался Дима. – Но в «балалайке» же все есть. Потому я сильно не переживал. Разберутся, думал. И разобрались.

Дима допил свой коньяк.

– Знаешь, – сказала Катя. – Что-то тут не то… Со смертью Заура. Ты, наверное, будешь смеяться, но я чувствую, что это не инфаркт. И не смерть от того, что он был от алкоголя зашит. Там что-то другое.

– Женщина, – улыбнулся Дима. – Женщины всегда что-то чувствуют. Что-то такое.

Тут у Димы пиликнул телефон.

Дима не торопился смотреть, кто там может беспокоить его в такое позднее время. Всем, кому надо, он уже позвонил. Дима разлил коньяк по бокалам, только потом поднял телефон со стола и прочитал, что ему написали.

После того, как Дима прочел сообщение, он побелел.

– Что там? – Катя увидела, как поменялся Дима в лице. Он молча протянул телефон девушке.

Катя приняла телефон и заглянула в экран.

Вместо телефона отправителя на экране светились какие-то символы, буквы и значки.

На экране же была короткая запись от неизвестного абонента.

«Привет, мои неожиданные друзья. Изаура пришел явить вам чудо».

Приглашаем авторов к участию в журнале «Вестник современных цифровых технологий»

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция принимает материалы статей, соответствующие тематике журнала, содержащие новые научные результаты, не опубликованные ранее и не предназначенные к публикации в других печатных или электронных изданиях. Проводится независимое внутреннее рецензирование. Статьи в журнале публикуются бесплатно (объем – до 15 тыс. знаков), после получения одобрения Редакционного совета.

Для опубликования статьи в редакцию журнала необходимо направить по адресу *accda@c3da.org, info@c3da.org* **следующие материалы в электронном виде:**

• рукопись статьи в DOC- и PDF-форматах;
• иллюстрации, предоставленные также и отдельными файлами в формате JPG или PNG с разрешением 72 dpi;
• сведения об авторах, содержащие фамилию, имя, отчество, ученые степень и звание, должность, место работы, контактные телефоны или E-mail;
• англоязычную информацию, содержащую название статьи, ФИО авторов, аннотацию и ключевые слова;
• редакция может запросить экспертное заключение о возможности публикации статьи в открытой печати.

ПОСЛЕДОВАТЕЛЬНОСТЬ МАТЕРИАЛОВ ДЛЯ ПУБЛИКАЦИИ:

1. шифр УДК (см. Справочник УДК) в левом верхнем углу;
2. название статьи (полужирным шрифтом по центру) не более 12 слов;
3. инициалы и фамилия автора (полужирным шрифтом по центру), к каждому автору- сноска, содержащая ученое звание, должность, название организации (без сокращений), e-mail;
4. Аннотация, излагающая суть работы и полученные результаты (5-7 строк);
5. ключевые слова (8-10 слов);
6. англоязычная информация по статье (по пп.2-5)
7. текст статьи с учетом указанных далее требований к его оформлению;
8. список литературы, оформленный по ГОСТ Р 7.0.5-2008.

Статья должна быть структурирована, т.е. должна включать разделы с названиями, кратко и точно отражающими их содержание, в том числе:

• введение, содержащее обоснование актуальности и краткий обзор проблематики;
• четкую постановку задачи исследования;
• описание метода решения задачи исследования;
• прикладную интерпретацию и иллюстрацию полученных результатов исследования;
• заключение, включающее обобщение и указание области применения полученных результатов, не повторяющее аннотацию и не ограничивающееся простым перечислением того, что сделано в работе.

С детальными требованиями к рисункам, таблицам, формулам, списку литературы, а также с примерами оформления статьи можно ознакомиться на странице Вестника http://c3da.org/journal.html.

Приглашается к сотрудничеству редактор для работы в редакции журнала по совместительству.
Просьба направлять резюме по электронному адресу *accda@c3da.org, info@c3da.org*

ТРЕБОВАНИЯ К РЕДАКТОРУ:

• отличное знание русского языка;
• свободное владение ПК, в том числе специальными текстовыми и графическими программами;
• опыт работы в издательстве.

Высшее техническое образование и знание английского языка являются существенными преимуществами.

ОБЯЗАННОСТИ

Редактор:
• редактирует рукописи, принятые к изданию;
• оказывает авторам необходимую помощь по улучшению структуры рукописей, выбору терминов, оформлению иллюстраций;
• проверяет, насколько учтены авторами замечания по доработке, предъявленные к рукописям;
• подписывает отредактированные рукописи в печать.